THE GOODYEAR EXPLOSION: ENSURING OUR NATION IS SECURE BY DEVELOPING A RISK MANAGEMENT FRAMEWORK FOR HOMELAND SECURITY

HEARING

BEFORE THE

SUBCOMMITTEE ON TRANSPORTATION SECURITY AND INFRASTRUCTURE PROTECTION

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

SECOND SESSION

JUNE 25, 2008

Serial No. 110–123

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.gpoaccess.gov/congress/index.html

U.S. GOVERNMENT PRINTING OFFICE

44–064 PDF WASHINGTON : 2008

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

LORETTA SANCHEZ, California
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
JANE HARMAN, California
PETER A. DEFAZIO, Oregon
NITA M. LOWEY, New York
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
JAMES R. LANGEVIN, Rhode Island
HENRY CUELLAR, Texas
CHRISTOPHER P. CARNEY, Pennsylvania
YVETTE D. CLARKE, New York
AL GREEN, Texas
ED PERLMUTTER, Colorado
BILL PASCRELL, JR., New Jersey
PETER T. KING, New York
LAMAR SMITH, Texas
CHRISTOPHER SHAYS, Connecticut
MARK E. SOUDER, Indiana
TOM DAVIS, Virginia
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
DAVID G. REICHERT, Washington
MICHAEL T. MCCAUL, Texas
CHARLES W. DENT, Pennsylvania
GINNY BROWN-WAITE, Florida
GUS M. BILIRAKIS, Florida
DAVID DAVIS, Tennessee
PAUL C. BROUN, Georgia
CANDICE S. MILLER, Michigan

I. LANIER LAVÁNT, *Staff Director & General Counsel*
ROSALINE COHEN, *Chief Counsel*
MICHAEL TWINCHEK, *Chief Clerk*
ROBERT O'CONNOR, *Minority Staff Director*

SUBCOMMITTEE ON TRANSPORTATION SECURITY AND INFRASTRUCTURE PROTECTION

SHEILA JACKSON LEE, Texas, *Chairwoman*

EDWARD J. MARKEY, Massachusetts
PETER A. DEFAZIO, Oregon
ELEANOR HOLMES NORTON, District of Columbia
YVETTE D. CLARKE, New York
ED PERLMUTTER, Colorado
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*
DANIEL E. LUNGREN, California
GINNY BROWN-WAITE, Florida
GUS M. BILIRAKIS, Florida
PAUL C. BROUN, Georgia
PETER T. KING, NEW YORK *(Ex Officio)*

MICHAEL BELAND, *Director & Counsel*
NATALIE NIXON, *Deputy Chief Clerk*
COLEY O'BRIEN, *Minority Senior Counsel*

CONTENTS

THE GOODYEAR EXPLOSION: ENSURING OUR NATION IS SECURE BY DEVELOPING A RISK MANAGEMENT FRAMEWORK FOR HOMELAND SECURITY

Wednesday, June 25, 2008

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON TRANSPORTATION SECURITY AND
INFRASTRUCTURE PROTECTION,
Washington, DC.

The subcommittee met, pursuant to call, at 2:33 p.m., in Room 311, Cannon House Office Building, Hon. Sheila Jackson Lee [Chairwoman of the subcommittee] presiding.

Present: Representatives Jackson Lee and Bilirakis.

Ms. JACKSON LEE [presiding]. The subcommittee will come to order.

The subcommittee is meeting today to receive testimony on the Goodyear explosion, ensuring our Nation is secure by developing a risk-management framework for homeland security. Our witnesses today will testify about the Department of Homeland Security's approach to risk management. In addition, we will hear a real-life story, real-life testimony on the tragedy of the Goodyear explosion that occurred in Houston exactly 2 weeks ago.

I offer to all of those who have been affected and all of those who have lost loved ones, in particular our witness on the second panel, our deepest and expressed and sincere sympathy.

I do want to indicate that my colleague, Congressman Green, was here earlier, and I would like to ask without objection that the gentleman from Texas, if he is able to arrive again, be authorized to sit for the purpose of questioning witnesses during the hearing today. Without objection, hearing none, it is so ordered.

Before I begin, there is always a moment of reflection and joy, and I do want to acknowledge the Calentar family. Mr. Perez and his nephew Mr. Calentar, if you all would stand? This young man is the recipient of the Artist Award from Wheaton High School in Houston, Texas. So we welcome him and we welcome his family, his sister, his brother, and his uncle. Thank you. You are all very welcome. Thank you very much.

[Applause.]

I am proud to convene today's hearing, which will focus on the Government's homeland security approach to risk management—a very key element of survival in this Nation. If you cannot manage risk, then you are ultimately unable to address the questions of

pending terrorist acts if they are to occur, and those unpredictable natural disasters.

Two weeks ago, there was a tragic accident at the Goodyear chemical plant in Houston, Texas. It is my belief that these types of incidents can be avoided if the appropriate risk management strategies are put in place. If the Department of Homeland Security can facilitate a comprehensive risk management program across the Federal Government and the private sector, it will go a long way toward preventing additional tragedies like the one that occurred in my own home town.

We are well aware that 85 percent of the critical infrastructure is in the hands of private entrepreneurs. Therefore, this must be a deeply embedded partnership in order for us to be able to save lives. In particular, I want to thank Mr. Raymond McInnis for his courage to testify here today after tragically losing his wife in the chemical explosion at the Goodyear plant on June 11. We thank him for his courage. His courage reminds us that we must push our Nation's chemical plants to take all of the necessary precautions to ensure that the American people are not put in unnecessary danger.

Mr. McInnis will address what this Government and our country's employers can do to keep events like the one at the Goodyear plant from happening. Again, Mr. McInnis, we thank you very much for being here today. We are well aware of the service of years that you have given to the Goodyear plant, so we are aware as well that in addition to your tragedy and your personal loss, you will give us a welcome knowledge and understanding. We are so grateful for your presence here today.

I would like to note that Goodyear declined our invitation to testify this afternoon. However, I have been assured that I will be kept informed of the developments related to its investigation of this serious matter. I have had an opportunity for discussion. Discussion must continue. The involvement must continue. We must find a way to ensure that these incidents do not occur.

The DHS must be on the frontlines of being preventive in preventing these tragedies however they may occur from happening to undermine the security and the safety of America. In no way is this hearing intended to influence an ongoing investigation. I encourage my colleagues to respect this fact as we attempt to learn about the need for a risk management framework for homeland security and how such a framework may apply to workers at chemical facilities.

Chairman Thompson, Ranking Member Lungren and I have taken a special interest in risk management. The reason for this is clear. Scarce Federal resources must be devoted to implementing meaningful homeland security strategies and programs designed to reduce risk from all hazards. I applaud Secretary Chertoff for espousing a risk-based approach to homeland security. Today, we are going to learn more about what that means and how it can be improved.

Our focus on risk cannot come at a more meaningful time. The threat posed by all types of hazards continues to endanger the American people. The resources to mitigate that threat must be allocated efficiently. We are in a budgetary situation that requires us to make difficult choices and to embrace a risk management strat-

egy that will help us make rational investment decisions with our homeland security dollars.

This subcommittee has sent three letters to the Department in an effort to understand its risk management practices. We have not been satisfied with many of its responses. Today, I look forward to getting answers from Under Secretary Jamison, who oversees many of the Department's risk-related programs.

Our approach to homeland security risk management must encompass all of the Federal departments and agencies, State and local governments, and the private sector. Today, we will hear from the Port Authority of New York and New Jersey. It has developed what I consider to be an effective risk management program. The more we learn about these types of successes, the more alternatives we have to choose from in adopting and promoting strategies at the Federal level.

I am fully aware that no methodology or analytical tool exists that will serve as a silver bullet. Indeed, there needs to be a baseline or set of principles that guides the Department's components so that they can develop new methods of risk analysis to support their activities.

I have many concerns about the Department's Office of Risk Management and Analysis. I believe we should increase the budget. It has yet to produce a baseline or a set of principles to guide the Department's risk management program. It has yet to justify its $10 million budget. I believe it will need more money. In order to do that, because risk management is so important, it is at the cutting edge of saving lives, we need to have the first baseline so we can make the argument for more funding.

Still more troubling is the fact that there is no clear legislative or executive mandate supporting this office. It is unclear to this subcommittee whether it has the necessary authority to do its job. In the shadow or in the sunrise of a pending new administration, this all points to being prepared during the transitional time. The fact that we have this transitional time is key to focus on this risk management question.

Today's discussion will not end here, but I hope it will encourage the Department to implement policies adequate for the task at hand. I look forward to hearing the opinions of our witnesses on a new risk management Presidential directive, the potential for a chief homeland security risk officers and national homeland security risk assessment, and how we can ensure that budget recommendations are based upon risk management principles.

Furthermore, we want to know where the Office of Risk Management and Analysis fits into the Department's risk management program.

Once again, I would like to thank everyone for their participation today. I look forward to hearing from our witnesses.

At this time, without objection, I would like to enter two documents into the record. The first is a statement submitted by Dr. Henry H. Willis of the RAND Corporation entitled "Challenges of Applying Risk Management to Terrorism Security Policy". The second is an April, 2008 report by GAO, "Highlights of a Forum: Strengthening the Use of Risk Management Principles in Homeland Security."

Hearing no objection, it is so ordered.*

Let me also indicate that at the conclusion of the opening statements, you will be entering into the record three documents. So let me correct the record and indicate that instead of two, we will have three. That is the additional statement that is now being presented to us by Goodyear. As I indicated, Goodyear was invited to testify, and this committee will keep an open record and also continue to the extent that legislation will probably generate it out of this hearing.

They declined to testify, Goodyear, at today's hearing because they indicated that it was inappropriate to testify at this time. As I have already informed you, we have no intention of interfering with a pending investigation, but we welcome Goodyear's future testimony. As I have indicated that it is appropriate, we are going to submit a statement from Goodyear for the record that I would like to include at this time if there is no objection.

Hearing no objection, their statement will be submitted and we appreciate the presence of their statement.

[The information follows:]

PREPARED STATEMENT OF JOSEPH COPELAND, VICE PRESIDENT, GOODYEAR TIRE AND RUBBER COMPANY

JUNE 25, 2008

Goodyear appreciates the opportunity to submit this brief statement for the record of the hearing before the House Subcommittee on Transportation Security and Infrastructure Protection of the Committee on Homeland Security entitled "The Goodyear Explosion: Ensuring Our Nation is Secure by Developing A Risk Management Framework for Homeland Security." We want to express our heartfelt condolences to the McInnis family and friends for their tragic loss, and to assure the committee, as we have the Chairwoman, our employees and our community, that we are cooperating fully with all ongoing investigations of the accident by our company and the Occupational Safety and Health Administration (OSHA) and will be available to discuss their findings when the investigations are complete. In light of the brief passage of time since the accident 14 days ago, and these ongoing investigations, it would be inappropriate for us to speculate at the hearing today. Since witnesses may be offering opinions on this matter at the hearing, we ask that the following brief statement by Goodyear be included in today's hearing record.

On the morning of June 11, an explosion occurred at the Goodyear chemical plant in Houston, killing longtime Goodyear associate Gloria McInnis and injuring six other workers. The explosion, which appears to have been caused by the buildup of pressure in a device called a heat exchanger, also resulted in the release of ammonia in the immediate vicinity and required us to evacuate associates and contractors from the entire site.

As required by our safety protocols, emergency response coordinators began accounting for everyone who was on site at the time of the explosion. In fact, Mrs. McInnis was an emergency response coordinator and therefore would not have been evacuated off the plant property, but would have worked with other coordinators to respond to the emergency. Unfortunately, the shift foreman responsible for accounting for Mrs. McInnis' whereabouts mistakenly attributed a telephone conversation he had with Mrs. McInnis moments before the explosion as occurring after the explosion. He wrongly marked Mrs. McInnis as accounted for and assumed she was attending to duties elsewhere on site. That incorrect assessment resulted in the Goodyear plant manager making an inaccurate statement to the public, and Goodyear and the plant manager sincerely apologize to the community and to the McInnis family in particular.

Later in the morning, it was deemed safe for associates to return to work in other areas of the plant, but not the area in the immediate vicinity of the explosion. When work crews were able to access that area and inspect it more thoroughly, they tragically found Mrs. McInnis' body.

*The documents have been retained in committee files.

During the course of the day, investigators from multiple agencies—OSHA, the Department of Homeland Security, the U.S. Chemical Safety and Hazard Investigation Board, the Texas Commission on Environmental Quality and others—visited the site or made inquiries. As this has been deemed an industrial accident and not a matter of homeland security, OSHA has assumed jurisdiction over the investigation. That investigation is ongoing, and Goodyear is cooperating fully.

Goodyear's Houston team was shaken to its core by Mrs. McInnis' death and the injuries to another Goodyear associate and several contractors. Mrs. McInnis was a well-liked and hard-working associate who had been with the company for 31 years. Like Mrs. McInnis, a high percentage of our associates in Houston have worked at the plant for decades and they know each other quite well. Goodyear immediately offered grief counseling services to all who needed it.

Despite some media reports to the contrary, Goodyear officials made multiple attempts to reach out to the family. After the McInnis family retained an attorney, the attorney required all attempts to communicate with the family go through him. Company officials extended their condolences and requested permission to attend the funeral. In addition, the company offered to pay for the funeral and to use its Government relations team to help get Mrs. McInnis' son returned from Iraq for the funeral. Our human resources department immediately began processing the necessary paperwork to ensure that the family members receive all the benefits that they are entitled to. Her coworkers created a memorial to Mrs. McInnis at the plant, held a plant-wide moment of silence in her memory and even collected donations for the family.

Goodyear itself is conducting an investigation into whether individuals adhered to our safety and security protocols before and after the explosion. At this point, we do know that our security system was not compromised and no unauthorized individuals were on the site at the time of the explosion.

As for safety protocols, Goodyear works hard to eliminate injuries of any degree through its "No One Gets Hurt" safety initiative. The initiative includes educating all associates about our safety protocols and conducting drills to ensure that associates know what they are to do in case of an emergency. In fact, the initiatives have been so successful that OSHA recordable incidents—meaning injuries of any type, large or small—at the Houston plant dropped from 67 in 2000 to just 7 last year. We have seen similar improvements company-wide, and we have set even more aggressive goals to reduce workplace accidents and injuries. This is another reason why Mrs. McInnis' death and the injuries to the other workers are so devastating to the Goodyear family.

Our investigation into what caused the pressure to buildup in the heat exchanger and the aftermath is continuing. Therefore, it is premature for us to speculate on the cause. We have committed to cooperating fully with the committee, and we will provide our findings at the appropriate time.

In the meantime, we are grateful that the last two injured workers have been released from local hospitals. And we again want to extend our apologies to our community for the mistaken initial reports and our heartfelt condolences to Mrs. McInnis' family and friends for their loss.

Ms. JACKSON LEE. I am also very pleased to, No. 1, share this podium with the distinguished gentleman from California, who is the Ranking Member, Mr. Lungren. As was indicated by his office, he has been detained because of an item that could not be removed. We will be looking forward to working with him.

I am more than pleased to have a very dedicated, committed, and very informed Member of the House, but also a respected Member of the Homeland Security Committee, and an equally respected Member of the Subcommittee on Transportation Security and Infrastructure Protection, to serve today as Ranking Member. The Chair now recognizes Mr. Bilirakis, the distinguished gentleman from Florida, for an opening statement.

Mr. BILIRAKIS. Thank you, Madam Chairwoman. I really appreciate it very much.

I am pleased that you have called this hearing to examine the use of risk management in homeland security. I am honored to be filling in for Ranking Member Lungren who could not be with us today.

I think it is important to acknowledge at the outset of this hearing that neither public nor private sector entities can protect everyone everywhere from everything at all times. The Government and others instead seek to accurately understand the nature of threats, vulnerabilities, and their potential consequences to better inform themselves and us of the smartest and most efficient ways to manage and reduce risk.

Congress has rightly directed Federal agencies to use a risk-based approach to help guide important decisions about policy and resource allocation. The results have been mixed at best. However, the Department of Homeland Security has made progress analyzing risk within certain critical sectors. The progress of these risk assessments differs across each sector and within the Department for comparing cross-sector risk. This is an area that clearly needs attention and improvement.

Federal policymakers and those we represent deserve to know whether we are using scarce public resources as wisely as possible to minimize risk and maximize security. To be fair, I am not sure whether anyone can reasonably be expected to definitely answer that question right now, but we surely need to.

I think we also must be especially sensitive to the roll that Congress plays in providing political obstacles to risk-based resource allocation and strategic thinking in this area. We each fight to represent our constituents as best as we can, and in that process zealously, and perhaps without the benefit of having the broadest possible perspective, direct and redirect funding and policy priorities in a manner that may be inconsistent with the most effective risk-based homeland security strategy.

In that regard, I am interested to hear the perspectives of today's witnesses on whether the Federal policies and investment priorities are properly aligned with those areas that are most vulnerable and in which an attack or natural catastrophe could have the greatest consequence on our homeland security. We should not simply be throwing money at problems without reasonable assurances objectively based in fact that we are actually reducing risk.

Before I conclude, I want to express my condolences to Mr. Raymond McInnis, whose wife Gloria was killed in the explosion at the Goodyear plant in Houston earlier this month. My heart goes out to him and the other victims of this tragedy.

Madam Chairwoman, I want to thank you again for calling this hearing to help shed more light on a critical component of our homeland security strategy. I look forward to hearing from our distinguished witnesses on this very important topic. Thank you again, Madam Chairwoman. I yield back the balance of my time.

Ms. JACKSON LEE. Let me thank the gentleman very much for his statement today, a very constructive statement as we lay the groundwork for this hearing.

Other Members of the subcommittee are reminded that under committee rules, opening statements may be submitted for the record.

It is my pleasure now to begin the testimony of the first witness, the witnesses on the first panel. Our first witness is Under Secretary Robert D. Jamison. Mr. Jamison is under secretary for the National Protection and Programs Directorate at the Department

of Homeland Security. In his capacity as under secretary, Mr. Jamison looks at the Department's integrated efforts to analyze, manage and reduce risk.

Prior to joining NPPD, Mr. Jamison served as deputy administrator at the Transportation Security Administration. Before joining DHS, Mr. Jamison served for over 3 years as a deputy administrator of the Federal Transit Administration at the Department of Transportation.

Our second witness, Mr. Norman Rabkin, is a managing director for homeland security and justice at the Government Accountability Office. Mr. Rabkin helped to host a comptroller general's forum on strengthening the use of risk management principles in homeland security on October 25, 2007. The forum convened a group of experts to address effective practices and the challenges Federal agencies face in applying risk management to homeland security, and actions that can strengthen homeland security risk management.

We believe that setting the framework on the challenges as we move forward in looking for the legislative reform, these witnesses are going to add very much to our discussion and our roadmap in going forward.

Without objection, the witnesses' full statements will be inserted in the record. I now ask each witness to summarize his statement for 5 minutes, beginning with Under Secretary Jamison.

Gentlemen, you are welcome.

STATEMENT OF ROBERT D. JAMISON, UNDER SECRETARY, NATIONAL PROTECTION AND PROGRAMS DIRECTORATE, DEPARTMENT OF HOMELAND SECURITY

Mr. JAMISON. Thank you, Chairwoman Jackson Lee and Congressman Bilirakis, for the opportunity to appear before you this afternoon to address the Department's implementation of risk management practices.

DHS is committed to applying a risk management framework across all homeland security efforts to prioritize our prevention, protection and resource efforts. The standup of the Office of Risk Management and Analysis within the National Protection and Programs Directorate and the longstanding collaboration on risk analysis and risk management across the Department bear out this commitment.

With approximately 95,000 miles of coastline, 1 million passengers arriving daily through our ports, 450 airports and thousands of other critical infrastructure assets, our homeland cannot be secured at every moment in every way against every possible threat. Instead, as a Nation, we must be able to determine what levels of risk are acceptable and prioritize our efforts.

As a result, the Department must adopt an approach of analyzing risk and using the information to devise the most effective ways to improve security. DHS components have long recognized the need to use risk analysis as a guide to decisionmaking. Eager to leverage DHS components' existing work, DHS has made it a priority for the new Office of Risk Management and Analysis to examine risk from a departmental perspective, working closely with each component with risk management responsibilities.

DHS's risk management architecture must allow for the diversity of operational environments in DHS, yet consistently generate reliable results that can be further utilized for strategic decisionmaking across the domain. It must be simultaneously flexible, yet robust.

Because DHS has multiple responsibilities with several unique operating environments, the Department-wide risk management architecture has to be flexible enough to allow for the development of customized component-level risk analysis by experts who know the characteristics of their mission space. For example, TSA's air domain risk analysis was developed by experts who understand the particulars of airports, airlines and the Nation's air space, while NPPD's chemical facility regulatory regime known as CFAS was developed by risk experts in DHS and the chemical industry.

On the other hand, DHS risk architecture needs to be robust enough to allow us to draw from those component analyses to inform decisionmaking at a strategic level. DHS seeks to create a structure that provides components with guidance to conduct those risk analyses, but does not constrain them with overly specific or rigid requirements, while providing the leaders of the Department comprehensive information to make resource and management decisions that are risk-based.

How are we going to unite these two competing requirements? First, we need to establish an integrated risk management framework. This framework will consist of the doctrine, principles, processes, guidance and information flows that will enable risk-informed and cost-effective decisionmaking at all levels. A properly executed risk management framework serves as a force multiplier because it enables better alignment of security priorities and resources to needs.

Next, we will conduct strategic integrated risk analyses. Integrated risk analyses defines a path forward, while leveraging the existing body of work that has already been completed or conducted within or outside the Department. These integrated analyses will put all the hard work DHS components have completed to date to work, and provide DHS leadership with a strategic look at risk across multiple mission areas. The ultimate goal is to fully integrate those strategic analyses into a larger planning and resource allocation process.

The principal vehicle for implementing these goals is the DHS steering committee that NPPD has established. The risk steering committee is comprised of risk analysis leaders from across the Department, and works to ensure collaboration, information sharing, and consensus building across the Department.

The committee is already working on several projects that support the development of the integrated risk management framework and the integrated strategic risk analysis. NPPD is confident this approach will reap the benefits of all the hard work that has already been completed in the area of risk analysis, while also delineating a strategic vision for risk management.

Finally, I would like to take a moment to offer my personal condolences to the McInnis family. Events such as the recent plant explosion in Houston weigh on all of us. Earlier, I mentioned CFAS, the chemical facility regulation that requires identification of high-

risk facilities that hold chemicals of interest, and the subsequent development of security measures.

As we implement CFAS, we are striving to manage the risks associated with chemical security across the country. Over the coming months, we will be requiring high-risk chemical facilities to determine their most critical security vulnerabilities and put strategies in place to address those vulnerabilities. This risk-based approach not only advances the security of chemical facilities, but will also contribute to the broader understanding of risk as we integrate those results across the Department.

Thank you for holding this hearing and for your attention to this critical area of risk management. I would be happy to answer any questions you might have.

[The statement of Mr. Jamison follows:]

PREPARED STATEMENT OF ROBERT D. JAMISON

JUNE 24, 2008

Thank you, Chairwoman Jackson Lee, and distinguished Members of the subcommittee. It is a pleasure to appear before you today to address the Department's implementation and execution of risk management practices. The Department of Homeland Security (DHS) is committed to the careful analysis of risk to inform a broad range of decisions. This commitment is demonstrated by the establishment of the Office of Risk Management and Analysis (RMA) within the National Protection and Programs Directorate (NPPD), the long-standing level of attention devoted to risk assessment and analysis within DHS components, and the collaboration in risk analysis across DHS components.

THE CHALLENGES

Secretary Chertoff has reiterated the theme that no one entity—public or private—can effectively protect every single person at every moment in every place against every threat. Rather, the approach that the Department, indeed the Nation as a whole, must adopt is one of analyzing risk and using that information to devise the most cost-effective way of managing risk and improving security.

In the context of homeland security, estimating risk includes characterization of three key factors: threats, vulnerabilities, and consequences. Terrorist threats can change rapidly and adapt to new security measures, making the estimation of threat extremely challenging. Vulnerabilities are usually quantifiable through subject matter expert judgment and "red team" exercises that probe for weaknesses, but they vary widely for different scenarios or types of attack. The direct consequences of an attack are fairly straightforward to calculate, but it is very difficult to quantify indirect consequences, potential cascading effects, and the impact on the public psyche. Last, integrating terrorism risk assessments with other all-hazard risk assessments, such as natural disasters, is difficult. For these reasons, and many others, risk management in homeland security remains a complex and arduous undertaking.

Given these complexities in conducting risk assessments, there are two priorities when designing an overarching risk architecture for the Department. These priorities are:

1. Allowing for the development of customized, component-level risk analyses by analysts who know the unique characteristics of their mission space and the decision needs of their leaders, and
2. Creating risk analysis guidelines and standards that will allow the Department to aggregate risk information across the broad spectrum of the DHS mission space to inform strategic decisionmaking.

The key challenge for DHS and RMA moving forward is to develop approaches and guidance materials that are both flexible and robust enough to accommodate these two priorities.

DHS' RISK MANAGEMENT VISION

The Department's approach to risk-informed decisionmaking has matured considerably over the past 5 years. It will continue to evolve as our understanding grows and as new analytic approaches are developed to deal with the complexities and uncertainties inherent in many of the risks for which DHS holds responsibility. De-

spite the progress already made, there is clearly much that remains to be done. The Department continues to focus on improving DHS risk assessment methodologies, advancing decision support tools, and identifying risk-related information gaps. For example:

- The Transportation Security Administration (TSA) has identified critical vulnerabilities within certain transportation modes, such as unattended railcars carrying Toxic Inhalation Hazards, and analyzes the mitigation of these vulnerabilities through the use of detailed metrics reports.
- The Office of Infrastructure Protection (IP) continuously tracks National Infrastructure Protection Plan (NIPP) implementation activities across all sectors. This allows IP to monitor the progress of establishing sector-specific risk management processes.
- The Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) conducts an annual risk assessment called the Strategic Homeland Infrastructure Risk Assessment (SHIRA) that spans across all Critical Infrastructure/Key Resource (CIKR) sectors.
- RMA has instituted a risk governance structure within the Department.
- The Federal Emergency Management Agency (FEMA) is modernizing flood maps to help communities improve their level of security from a natural disaster through smart building and setting of construction standards to create safer housing.
- The Office of Health Affairs is relying on risk assessments conducted by the Science and Technology Directorate to guide all of our bio-defense countermeasure strategies—both medical and nonmedical—and to inform our policies.

In all of these examples, DHS and its components are improving the Department's ability to develop information about risks and use this information to inform decisions. To advance these efforts, and to leverage the expertise, the Department must continue to further the integration efforts. Based on this key challenge, RMA, in collaboration with the Department's components, has developed a vision to support the Department's efforts to advance its risk management capabilities. The vision is twofold:

1. Establish and institutionalize an integrated risk management framework. This framework will consist of the doctrine, principles, processes, guidance, and information flows that will enable risk-informed and cost-effective decisionmaking within components and at the DHS headquarters level. A properly executed risk management framework effectively serves as a force multiplier, as it enables better alignment of security priorities and resources to needs.
2. Conduct strategic, integrated risk analysis. We must be informed, at the strategic level, by an integrated departmental risk assessment. The integrated risk assessment should leverage the various risk analyses being conducted within and outside the Department.

An integrated risk management framework will help better ensure that these efforts are harmonized and work from the same principles and understanding. Strategic, cross-component analysis will leverage the advances DHS' components have made with regard to risk management while incorporating those advances into DHS' larger planning and resource allocation processes.

CURRENT RISK MANAGEMENT PRACTICES

The Department is tasked with fulfilling missions that range from finding persons lost at sea to detecting renegade nuclear weapons. Without a clear understanding of the risks facing our society, decisionmaking could become less effective. Our resources could be spent to protect the Nation against risks that are less significant, while we simultaneously fail to protect the Nation against the risks that are more critical.

NPPD, through RMA, is continuing to build the foundation for sound risk management practices across the Department. To enable the sharing and integration of RMA and component risk-related efforts, RMA has implemented a risk governance process within the Department. Central to this risk governance process is the DHS Risk Steering Committee (RSC) that RMA established. The RSC is comprised of risk analysis leads from across the Department and meets on a monthly basis. This approach ensures that there is collaboration, information-sharing, and consensus-building across the Department as we identify guidelines and recommendations for risk management and analysis. Currently, there are three working groups within the RSC. The efforts of the RSC working groups will provide the foundation for the integrated risk management framework and for strategic, cross-component analysis.

- *The Risk Assessment Process for Informed Decision-Making (RAPID) Working Group*.—RAPID is a strategic-level, Department-wide process that will assess

risk and inform strategic planning, programming, budgeting, and execution processes. The process is focused on developing techniques to evaluate the risk reduction impacts of relevant DHS programs.

- *The Lexicon Working Group*.—The lexicon is a comprehensive glossary of words and terms relevant to the practice of homeland security risk management that will be used to ensure better understanding of risk management terminology throughout the homeland security organization.
- *The Best Practices Working Group*.—The product is an inventory of risk management lessons learned and recommended procedures and guidelines that will be used to guide the components to ensure that the Department's risk methods are coherent, consistent, and technically sound.

The RSC has also been a very useful means for DHS components to coordinate their risk management efforts with each other. Examples of the programs that have RSC representation and participation include:

- IP's NIPP Risk Management Framework and its work with Federal/State/local/tribal partners in setting and pursuing CIKR protection goals and the establishment of Risk Integration and Analysis programs;
- The United States Coast Guard's (USCG) Maritime Security Risk Analysis Model (MSRAM), which allows USCG to develop and aggregate risk information at the port, sector, area, and national levels, and which supports numerous Coast Guard/DHS planning and resource allocation efforts at the strategic, operational, and tactical levels;
- The Office of Science and Technology's risk model, which analyzes the risk-reduction potential of various research and development initiatives.
- The Federal Emergency Management Agency's (FEMA) grant programs that utilize a risk-informed approach by considering both the risk profiles of specific jurisdictions and the quality of the business cases that the grant applicants develop to mitigate the risk.
- TSA's agent-based risk simulation model, called the Risk Management Analysis Tool, which takes into account that terrorists are a dynamic and adaptive adversary and allows TSA to identify the risk reduction value of any single layer of security within the U.S. aviation system.

These component efforts demonstrate both the quality and diversity of risk management efforts within DHS. The goal of RMA is not to mandate that DHS components use a certain tool or analytical technique to conduct their specific risk analyses. Instead, RMA is serving as the bridge to connect these existing efforts together and is building products and collaboration forums to better ensure they are harmonized moving forward. The DHS integrated risk management framework will embrace a wide range of analytical tools and techniques. Most importantly, the framework will help ensure that all DHS risk analysis efforts are transparent, defensible, and documented. It will also help ensure that these analyses can be leveraged for strategic, cross-component analysis at the DHS headquarters level.

Lastly, the RSC is a primary formal mechanism for the internal sharing of DHS risk information. However, a number of key external communications mechanisms are also in place at DHS because a critical part of the Department's risk management practices is how it communicates and works with its State, local, and tribal partners. For example, through the NIPP, DHS has established a framework that enables stakeholders from the private sector and public sector to coordinate on risk management issues. Government Coordinating Councils and Sector Coordinating Councils have been established across all CIKR sectors. Active information exchange occurs through the councils and through the Homeland Security Information Network. As the integrated risk management framework is developed, it will be shared with Federal, State, local, tribal and private sector stakeholders through these and other mechanisms that RMA is currently assessing.

ADVANCING RISK MANAGEMENT AT DHS

While we have made significant progress in our efforts to build an integrated, effective, and harmonized architecture for risk management at the Department, we are still in the early stages of a long journey. As a Department, we are striving to implement an approach where major decisions about investments, budgets, grants, planning priorities, operational posture, and security priorities are risk informed. To do so, we are moving toward an integrated framework of risk-informed decision-making where:

1. Decisions are framed to include an understanding of the risks associated with them;
2. Risks are identified, analyzed, communicated and assessed, so as to ensure we fully understand the nature of the problems we are trying to manage;

3. Alternative strategies for risk management are developed and analyzed for costs and benefits;
4. Decisions amongst these strategies are made with the best understanding of how they impact the risk; and
5. Decisions are monitored and reviewed so as to understand how they mitigated the risk.

Such a risk management process for decisionmaking will be applied across DHS to address strategic, operational, and tactical risks. As we move forward, the Department, through RMA and the RSC, expects to make this process the center of an integrated risk management framework.

In addition, DHS will continue to build the foundational efforts necessary to execute the framework and strategic analyses. These efforts will include the development of a risk management training and education program for both risk analysts and senior leaders, investment in new technologies for risk data collection, improved Department-wide access to resources for modeling and simulation, and the identification of useful risk management metrics.

CONCLUSION

As noted in the 2007 National Strategy for Homeland Security, the assessment and management of risk underlies the full spectrum of our homeland security activities, including decisions about when, where, and how to invest in resources that eliminate, control, or mitigate risk. We at DHS recognize that risk management within the context of homeland security is an evolving field. We know that there are improvements that we can make in applying risk management and analysis to support our decisionmaking. We rely on collaboration with experts inside and outside the Government to learn how we can improve our abilities to understand, communicate about, and manage risk.

Managing risk depends on accepting uncertainty; managing risk does not mean eliminating it. At DHS our goal with regard to risk management is to continually improve our ability to understand and recognize those risks, while developing the processes and methods that allow us to use that information to make better decisions. Those decisions govern how we invest our efforts in increasing preparedness, protection, and, ultimately, homeland security.

Thank you for holding this important hearing. I would be happy to respond to any questions you might have.

Ms. JACKSON LEE. Thank you, Secretary Jamison.

Mr. Rabkin, we thank you for your testimony.

STATEMENT OF NORMAN J. RABKIN, MANAGING DIRECTOR, HOMELAND SECURITY AND JUSTICE, GOVERNMENT ACCOUNTABILITY OFFICE

Mr. RABKIN. Madam Chairwoman, Mr. Bilirakis, and other Members of the subcommittee, thank you for inviting me to participate in today's hearing on the use of risk management principles in homeland security.

The Congress, the President, and the Department all recognize that the Federal Government can never assure complete security, and it certainly can't afford to invest unlimited resources trying to do so. Using risk as a basis to intelligently allocate relatively limited resources makes sense. How to do it is much more difficult.

Even before September 11, 2001, GAO was looking at how Federal agencies could make investment decisions based on risk. We created a conceptual framework for this decision process. We have displayed that in this graphic to my right and your left. This begins with identifying a program's goals, then assessing the risks, evaluating potential alternatives to mitigate the risks, deciding which alternatives in which to invest, and finally implementing the decision and monitoring the results of the investment, as well as any changes in goals and risks.

As you mentioned, last year we invited about two dozen international experts to the GAO to discuss how to strengthen the use of risk management principles in homeland security. My written statement summarizes the results of that session. Here are some of the highlights.

The participants first identified effective public and private sector risk management practices. For example, participants discussed the private sector's use of a chief risk officer, an executive responsible for focusing on understanding information about risks and reporting this information to other senior-level managers.

They also discussed examples of public sector organizations that have effectively integrated risk management practices into their operations, such as the U.S. Coast Guard, and compared and contrasted public and private sector risk management practices.

Then the participants identified four key challenges to applying risk management to homeland security. Many participants agreed that improving risk communication posed the greatest challenge to using risk management principles. More specifically, they cited the need to first establish a common lexicon for discussing risk; second, educating policymakers and the public about risks and engage in public discourse to reach consensus on acceptable levels of risk; and third, developing new risk communication practices to alert the public during emergencies.

The second challenge they cited were political obstacles to risk-based resource allocation. They discussed the reluctance of politicians and others to make risk-based funding decisions. Participants noted that elected officials' investment priorities are informed by the public's beliefs about which risks should be given the highest priority—beliefs that are often based on incomplete information.

As a result, the participants felt that there was less incentive for officials to invest in long-term opportunities to reduce risk, such as investing in specific border security assets or transportation infrastructure, when the public may not view these investments as addressing a perceived risk.

The third challenge is in the area of strategic thinking. They commented that a better national strategic planning process is needed to guide Federal investments in homeland security, one that more explicitly involves discussions of tradeoffs of investing in programs that protect against one risk rather than another. They also suggested that fragmented approaches within and across the Federal Government be addressed by developing Government-wide guidance on using risk management principles.

The final challenge they discussed was related to developing public-private partnerships. They believe that risk management is the responsibility of both the public and the private sectors. They suggested that public-private collaboration would be improved if representatives from State and local governments, as well as the private sector, were more involved in public risk assessments and had more access to the Federal Government's information about threats, vulnerabilities and consequences, and this information being used to assess these various risks.

The challenges that our participants cited are consistent with the goals and strategies of the National Infrastructure Protection Plan.

Our sense is that DHS also recognizes them and is organizing itself to deal with them.

This concludes my statement. I would be pleased to answer any questions you or the subcommittee Members may have.

[The statement of Mr. Rabkin follows:]

PREPARED STATEMENT OF NORMAN J. RABKIN

JUNE 25, 2008

GAO HIGHLIGHTS

Highlights of GAO–08–904T, a testimony before the Subcommittee on Transportation Security and Infrastructure Protection, Homeland Security Committee, House of Representatives.

Why GAO Convened This Forum

From the terrorist attacks of September 11, 2001, to Hurricane Katrina, homeland security risks vary widely. The Nation can neither achieve total security nor afford to protect everything against all risks. Managing these risks is especially difficult in today's environment of globalization, increasing security interdependence, and growing fiscal challenges for the Federal Government. Broadly defined, risk management is a process that helps policymakers assess risk, strategically allocate finite resources, and take actions under conditions of uncertainty.

GAO convened a forum of 25 national and international experts on October 25, 2007, to advance a national dialog on applying risk management to homeland security. Participants included Federal, State, and local officials and risk management experts from the private sector and academia.

Forum participants identified: (1) What they considered to be effective risk management practices used by organizations from the private and public sectors; and (2) key challenges to applying risk management to homeland security and actions that could be taken to address them. Comments from the proceedings do not necessarily represent the views of all participants, the organizations of the participants, or GAO. Participants reviewed a draft of this report and their comments were incorporated, as appropriate.

RISK MANAGEMENT: STRENGTHENING THE USE OF RISK MANAGEMENT PRINCIPLES IN HOMELAND SECURITY

What Participants Said

Forum participants identified what they considered to be effective public and private sector risk management practices. For example, participants discussed the private sector use of a chief risk officer, though they did not reach consensus on how to apply the concept of the chief risk officer to the public sector. One key practice for creating an effective chief risk officer, participants said, was defining reporting relationships within the organization in a way that provides sufficient authority and autonomy for a chief risk officer to report to the highest levels of the organization. Participants stated that the U.S. Government needs a single risk manager. One participant suggested that this lack of central leadership has resulted in distributed responsibility for risk management within the administration and Congress and has contributed to a lack of coordination on spending decisions. Participants also discussed examples of public sector organizations that have effectively integrated risk management practices into their operations, such as the U.S. Coast Guard, and compared and contrasted public and private sector risk management practices.

According to the participants at our forum, three key challenges exist to applying risk management to homeland security: improving risk communication, political obstacles to risk-based resource allocation, and a lack of strategic thinking about managing homeland security risks. Many participants agreed that improving risk communication posed the single greatest challenge to using risk management principles. To address this challenge, participants recommended educating the public and policymakers about the risks we face and the value of using risk management to establish priorities and allocate resources; engaging in a national discussion to reach a public consensus on an acceptable level of risk; and developing new communication practices and systems to alert the public during an emergency. In addition, to address strategic thinking challenges, participants recommended the Government develop a national strategic planning process for homeland security and Government-wide risk management guidance. To improve public-private sector coordination, forum participants recommended that the private sector should be more involved in

the public sector's efforts to assess risks and that more State and local practitioners and experts be involved through intergovernmental partnerships.

Madam Chairwoman and Members of the subcommittee: Thank you for inviting me to participate in today's hearing on the use of risk management principles in homeland security. As shown by the terrorist attacks of September 11, 2001, and Hurricane Katrina, homeland security risks vary widely. The Nation can neither achieve total security nor afford to protect everything against all risks. Managing these risks is especially difficult in today's environment of globalization, increasing security interdependence, and growing fiscal challenges for the Federal Government. It is increasingly important that organizations effectively target homeland security funding—totaling nearly $65 billion in 2008 Federal spending alone—to address the Nation's most critical priorities.

Using principles of risk management can help policymakers reach informed decisions regarding the best ways to prioritize investments in security programs so that these investments target the areas of greatest need. Broadly defined, risk management is a strategic process for helping policymakers make decisions about assessing risk, allocating finite resources, and taking actions under conditions of uncertainty. The Department of Homeland Security (DHS) has established a risk management framework to help the Department target its investments in security programs based on risk. This framework defines risk as a function of threat, vulnerability, and consequence, or, in other words, a credible threat of attack on a vulnerable target that would result in unwanted consequences.

Our prior work has shown that using risk management principles to prioritize which programs to invest in and to measure the extent to which such principles mitigate risk is a challenging endeavor. For this reason, to assist both Congress and Federal agencies, including DHS, GAO convened an expert panel to advance the national dialog on strengthening the use of risk management principles to manage homeland security programs. Today, I'll discuss the highlights of our panel's thoughts on the issues we asked them to identify: (1) Effective risk management practices used by organizations from the public and private sectors; and (2) key challenges faced by public and private organizations in adopting and implementing a risk-based approach to manage homeland security programs and actions that could be taken to address them.

SUMMARY

Participants identified effective public and private sector risk management practices. For example, participants discussed the private sector use of the chief risk officer. However, participants discussed but did not reach consensus on how to apply this concept of a chief risk officer to the public sector. They also discussed examples of public sector organizations that have effectively integrated risk management practices into their operations, such as the U.S. Coast Guard, and compared and contrasted public and private sector risk management practices.

According to the participants at our forum, three key challenges exist to applying risk management to homeland security: improving risk communication, political obstacles to allocating resources based on a consideration of risk, and a lack of strategic thinking about managing homeland security risks. Many participants, 35 percent, agreed that improving risk communication posed the single greatest challenge to using risk management principles. Further, 19 percent of participants stated political obstacles to risk-based resource allocation was the single most critical challenge, and the same number of participants, 19 percent, said the single most critical challenge was a lack of strategic thinking. The remaining participants identified other key challenges, for example, technical issues such as the difficult but necessary task of analyzing threat, vulnerability, and consequences of a terrorist attack in order to assess risk; partnership and coordination challenges; and the need for risk management education.

The expert panel also identified ways to address some of these challenges. To better communicate about risks, participants recommended that we educate the public and policymakers about the risks we face and the value of using risk management to establish priorities and allocate resources; engage in a national discussion to reach a public consensus on an acceptable level of risk; and develop new communication practices and systems to alert the public during an emergency. To better allocate resources based on risk, participants recommended that public officials and organizations consider investing in protective measures that yield long-term benefits. In addition, to address strategic thinking challenges, participants recommended the Government develop a national strategic planning process for homeland security and Government-wide risk management guidance. To improve public-private sector coordination, forum participants recommended that the private sector should be

more involved in the public sector's efforts to assess risks and that more State and local practitioners and experts be involved through intergovernmental partnerships.

BACKGROUND

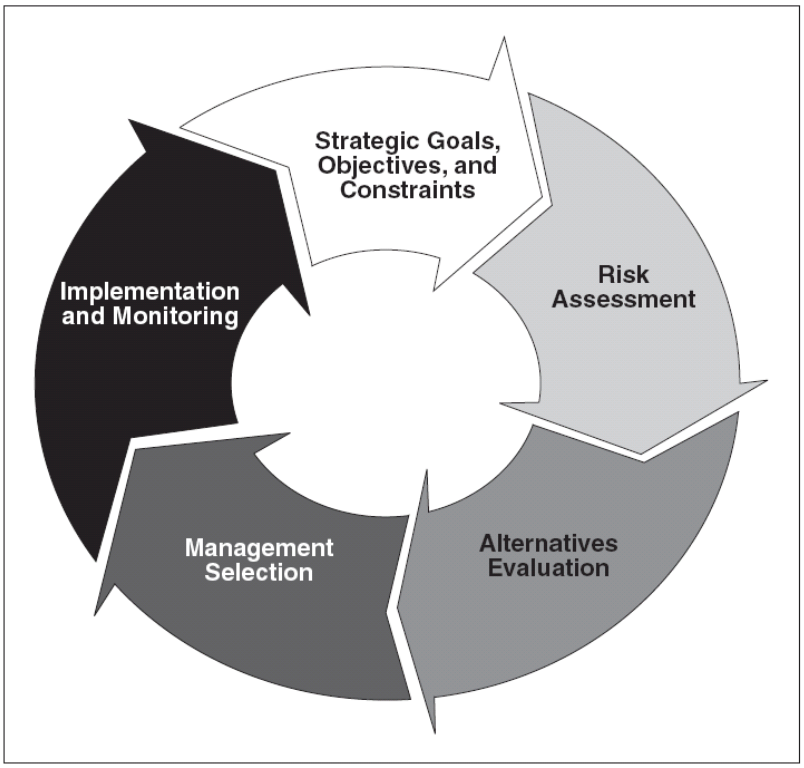
The Comptroller General convened this expert panel from the United States and abroad to advance a national dialog on strengthening the use of risk management principles to better manage homeland security programs. The forum brought together a diverse array of experts from the public and private sectors, including, from the public sector, a former Governor, a former DHS under secretary, a U.S. Coast Guard Admiral, and senior executives from DHS, the U.S. Army, and the National Intelligence Council, as well as State and local officials with homeland security responsibilities. From the private sector, participants included executives from leading multinational corporations such as Swiss Re, Westfield Group, JPMorgan Chase, and Wal-Mart. In addition, several of the world's leading scholars from major universities, the National Research Council, and the RAND Corporation participated in the forum. (See app. I for a list of participants.)

Recognizing that risk management helps policymakers make informed decisions, Congress and the administration have charged Federal agencies to use a risk-based approach to prioritize resource investments. Nevertheless, Federal agencies often lack comprehensive risk management strategies that are well integrated with program, budget, and investment decisions. To provide a basis for analyzing these strategies, GAO has developed a risk management framework [1] based on industry best practices and other criteria. This framework, shown in figure 1, divides risk management into five major phases: (1) setting strategic goals and objectives, and determining constraints; (2) assessing risks;[2] (3) evaluating alternatives for addressing these risks; (4) selecting the appropriate alternatives; and (5) implementing the alternatives and monitoring the progress made and results achieved.

[1] For a description of this framework, see Appendix I of GAO, *Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure,* GAO–06–91 (Washington, DC: Dec. 15, 2005).

[2] Risk assessment is the process of qualitatively or quantitatively determining the probability of an adverse event and the severity of its impact on an asset.

Figure 1: GAO Risk Management Framework



Source: GAO.

Our work has indicated that while DHS is making progress in applying risk management principles to guide its operational and resource allocation decisions, challenges remain. GAO has assessed DHS's risk management efforts across a number of mission areas—including transportation security, port security, border security, critical infrastructure protection, and immigration enforcement—and found that risk management principles have been considered and applied to varying degrees. For example, in June 2005 we reported that the Coast Guard had developed security plans for seaports, facilities, and vessels based on risk assessments.[3] However, other components had not always utilized such an approach. As we reported in August 2007, while the Transportation Security Administration has developed tools and processes to assess risk within and across transportation modes, it had not fully implemented these efforts to drive resource allocation decisions.[4] Moreover, in February 2007, we reported that DHS faced substantial challenges related to strengthening its efforts to use information on risk to inform strategies and investment decisions, for example, by integrating a consideration of risk into annual budget and program review cycles.[5] We also reported that while integrating a risk management approach into decisionmaking processes is challenging for any organization, it is particularly difficult for DHS given its diverse set of responsibilities. The Department is responsible for dealing with all-hazards homeland security risks—ranging from natural disasters to industrial accidents and terrorist attacks. The history of

[3] GAO, *Strategic Budgeting: Risk Management Principles Can Help DHS Allocate Resources To Highest Priorities,* GAO–05–824T (Washington, DC: June 29, 2005).
[4] GAO, *Department of Homeland Security: Progress Report on Implementation of Mission and Management Functions,* GAO–07–454 (Washington, DC: Aug. 17, 2007).
[5] GAO, *Homeland Security: Applying Risk Management Principles to Guide Federal Investments,* GAO–07–386T (Washington, DC: Feb. 7, 2007).

natural disasters has provided experts with extensive historical data that are used to assess risks. By contrast, data about terrorist attacks are comparatively limited, and risk management is complicated by the asymmetric and adaptive nature of our enemies.

In addition to helping Federal agencies like DHS focus their efforts, risk management principles can help State and local governments and the private sector—which owns over 85 percent of the Nation's critical infrastructure—prioritize their efforts to improve the resiliency of our critical infrastructure and make it easier for the Nation to rebound after a catastrophic event. Congress has recognized State and local governments and the private sector as important stakeholders in a national homeland security enterprise and has directed Federal agencies to foster better information sharing with these partners. Without effective partnerships, the Federal Government alone will be unable to meet its responsibilities in protecting and securing the homeland. A shared national approach—among Federal, State, and local governments as well as between public and private sectors—is needed to manage homeland security risk.

IDENTIFYING EFFECTIVE RISK MANAGEMENT PRACTICES IN THE PRIVATE AND PUBLIC SECTORS

Participants discussed effective risk management practices used in the public and private sector. For example, they discussed the concept of a chief risk officer but did not reach consensus on how to apply the concept to the public sector. The participants also identified examples of public sector organizations that effectively integrated risk management into their operations and compared and contrasted public and private sector risk management practices.

Chief Risk Officer

Participants said that private sector organizations have established the position of the chief risk officer, an executive responsible for focusing on understanding information about risks and reporting this information to senior executives. One key practice for creating an effective chief risk officer, participants said, was defining reporting relationships within the organization in a way that provides sufficient authority and autonomy for a chief risk officer to report to the highest levels of the organization. However, participants did not reach consensus on how to apply the concept of the chief risk officer to the public sector. Participants stated that the U.S. Government needs a single risk manager. One participant suggested that this lack of central leadership has resulted in distributed responsibility for risk management within the administration and Congress and has contributed to a lack of coordination on spending decisions.

Another participant stated that the Secretary of DHS fills the chief risk officer role. Participants identified various challenges associated with appointing a chief risk officer within the public sector, including: (1) Balancing the responsibilities for protection against seizing opportunities for long-range risk reduction; (2) creating a champion but not another silo that is not integrated with other components of the organization; and (3) generating leadership support for the position.

Integration of Risk Management Principles into Public Sector Operations

Participants identified examples of organizations that effectively integrated risk management into the operations of public sector organizations, including the U.S. Coast Guard, the U.S. Army Corps of Engineers, and the Port Authority of New York and New Jersey. Participants stated that the Coast Guard uses risk management principles to allocate resources, balance competing needs of security with the efficient flow of commerce, and implement risk initiatives with its private sector partners, for example, through Area Maritime Security Committees. According to another participant, the Army Corps developed flood risk management practices that he saw as notable because this information was used to digest and share critical information with the public. One participant noted that the Port Authority of New York and New Jersey developed and implemented a risk assessment program that guided the agency's management in setting priorities for a 5-year, $500 million security capital investment program. According to this participant, this methodology has since been applied to over 30 other transportation and port agencies across the country, and the Port Authority has moved from conducting individual risk assessments to implementing an ongoing program of risk management.

Comparing and Contrasting Public and Private Sector Risk Management Practices

Participants observed that while, in some instances, the public and private sector should apply risk management principles in similar ways, in other instances, the public and private sectors manage risk differently. One participant stated in both

the public and private sectors the risk management process should include the systematic identification and assessment of risks through scientific efforts; efforts to mitigate risks; and risk adaptation to address financial consequences or to allow for effective transfer of risk. However, participants noted that the private and public sectors also manage risk differently. One participant said the private sector manages risk by "pre-funding" and diversifying risk through insurance. In addition, the private sector creates incentives for individuals to lower the risks they face from, for example, a car accident or a natural disaster, by offering to reduce insurance premiums if the policy holder takes certain steps to mitigate these risks. Similarly, the public sector also plays a unique role in managing risk, for instance, regulating land use and establishing building codes; organizing disaster protection, response, and recovery measures; setting regulatory frameworks; and supplementing the insurance industry.

In addition, participants noted that the private sector organizations have more flexibility than the public sector to select which risks to manage. For instance, participants stated that the private sector could avoid risks in cases where the costs of ensuring these risks are too high. Additionally, a participant noted that the private sector tends to naturally consider opportunity analysis—or the process of identifying and exploring situations to better position an organization to realize desirable objectives—as an important part of risk management. In contrast, participants observed, public sector organizations have less flexibility to select which risks to address through protective measures. Like the private sector, the Government has to makes choices about which risks to protect against—since it cannot protect the Nation against all hazards. Unlike the private sector, the Government has a wide responsibility for preparing for, responding to, and recovering from all acts of terrorism and natural or manmade disasters and is accountable to the public for the investment decisions it makes.

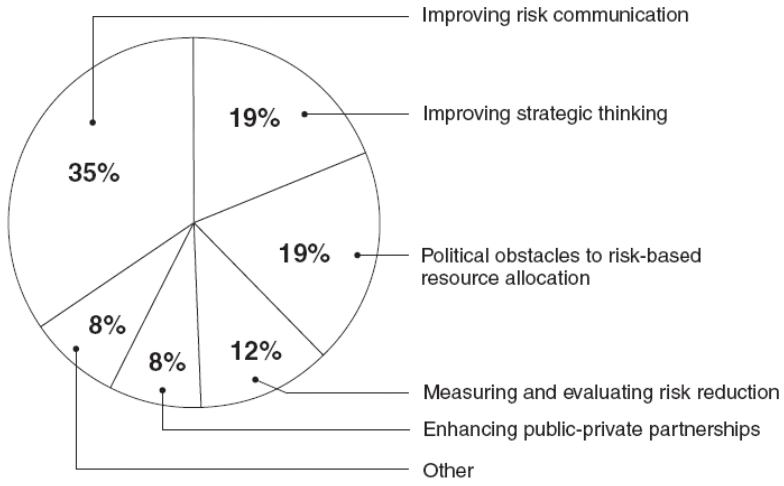
IDENTIFYING AND ADDRESSING THE MOST CRITICAL HOMELAND SECURITY RISK MANAGEMENT CHALLENGES

Participants identified three key challenges to strengthening the use of risk management in homeland security—risk communication, political obstacles to making risk-based investments, and a lack of strategic thinking. Participants also recommended ways to address them.

Key Challenges

Many participants, 35 percent, agreed that improving risk communication posed the single greatest challenge to using risk management principles (see fig. 2 below). Further, 19 percent of participants stated political obstacles to risk-based resource allocation was the single most critical challenge, and the same proportion of participants, 19 percent, said the single most critical challenge was a lack of strategic thinking. The remaining participants identified other key challenges, for example, technical issues such as the difficult but necessary task of analyzing threat, vulnerability, and consequences of a terrorist attack in order to assess and measure risk reduction; and partnership and coordination challenges.

Figure 2: Key Challenges in Applying Risk Management to Homeland Security



Source: GAO analysis of participants' forum polling responses.

Risk Communication Challenges

Participants identified several risk communication challenges and recommended actions to address them as follows:

- *Educate the public about risks and engage in public discourse to reach consensus on an acceptable level of risk*.—Participants said that the public lacks a fact-based understanding of what homeland security risks the Nation faces. Participants attributed these problems to media coverage that undermines a fact-based public discussion of risk by sensationalizing acts of terrorism that have dramatic consequences but may be unlikely to occur. In addition, participants stated that even though it is not possible to prevent all disasters and catastrophes, public officials need to engage the public in defining an acceptable level of risk of a terrorist attack or natural disaster in order to make logical, risk-based resource allocation decisions. To communicate with the public about risks in a meaningful way, participants recommended educating the public on how risk is defined, providing fact-based information on what risks we face and the probability they might occur, and explaining how risk informs decisionmaking. One expert recommended the Government communicate about risks through public outreach in ways that calms the public's fears while raising awareness of risks. Another participant recommended that the country engage in a national public discourse to reach consensus on an acceptable level of risk.
- *Educate policymakers and establish a common lexicon for discussing risk*.—Participants emphasized the importance of educating elected officials on risk management. Several participants believed that the distinction between risk assessment—involving scientific analysis and modeling—and risk management—involving risk reduction and evaluation—is not widely understood by policymakers. In addition, one expert also noted that the Nation should do more to train a cadre of the next generation of risk management professionals. Given differences in education and levels of understanding about risk management, the participants felt it would be important to develop a common lexicon that can be used for dialog with both the layman and the subject matter expert. Without a common, shared understanding of risk management terms, communicating about risks is challenging. Some members of our expert panel recommended focusing specifically on educating elected officials and the next generation of policymakers about risk management. One participant pointed out that a new administration and Congress will soon enter office with a new set of policy objectives, and it will be important to highlight the importance of risk management to incoming policymakers and to persuade them to discuss it. Panelists also rec-

ommended creating a common vocabulary or lexicon that defines common risk management terms.

- *Develop new risk communication practices to alert the public during emergencies*.—Participants said that Government officials lack an understanding of what information to share and how to communicate with the public during an emergency. Participants said that risk analysis, including predictive modeling, tends to neglect a consideration of how the public's expectations and emotions can impact the effectiveness of response efforts and affect the likelihood the public will respond as predicted or directed by Government officials during an emergency. According to one participant, Hurricane Katrina demonstrated that the efficacy of emergency response efforts depends on how the public behaves, as some people chose to shelter in place while others followed directions to evacuate. Participants recommended that governments consider what information should be communicated to the public during a crisis and how best to communicate that information. For instance, one participant suggested that experts look at existing risk communication systems, such as the National Weather Service, that could be used as models for a homeland security risk communication system. The participant noted that the service provides both national and local weather information, looks at overall risks, and effectively provides actionable information to be used by both the public and private sectors. Participants criticized the current color-coded DHS Homeland Security Advisory System as being too general, suggesting that the public does not understand what is meant by the recommended actions such as being vigilant.

Political Obstacles to Risk-Based Resource Allocation

Participants said political obstacles pose challenges to allocating homeland security resources based on risk. Participants identified the reluctance of politicians and others to make risk-based funding decisions. Participants noted that elected officials' investment priorities are informed by the public's beliefs about which risks should be given the highest priority, beliefs that are often based on incomplete information. As a result, participants stated that there is less incentive for officials to invest in long-term opportunities to reduce risk, such as investing in transportation infrastructure, when the public does not view these investments as addressing a perceived risk. To better allocate resources based on risk, participants recommended that public officials and organizations consider investing in protective measures that yield long-term benefits.

Need to Improve Strategic Thinking

Participants agreed that a lack of strategic thinking was a key challenge to incorporating risk-based principles in homeland security investments. In particular, participants noted that challenges existed in these areas:

- *A national strategic planning process is needed to guide Federal investments in homeland security*.—Participants said there is a lack of a national strategic planning process to guide Federal investments in homeland security. Balancing the security concerns of various Federal Government agencies that have diverse missions in areas other than security, such as public safety and maintaining the flow of commerce, poses a significant strategic challenge, some participants stated. One participant stated that the President had developed a strategy to guide, organize, and unify the Nation's homeland security efforts in the October 2007 National Strategy for Homeland Security. However, several other participants said that a better process is needed for strategic planning. For example, to think strategically about risk they recommended that stakeholders discuss tradeoffs, such as whether more resources should be spent to protect against risks from a conventional bomb, nuclear attack, biological attack, or a hurricane. Another participant noted that the purpose of risk assessment is to help answer these strategic questions. One participant also recommended that the short-term goal for a national strategic planning process should be identifying the big problems that strategic planning needs to address, such as measuring the direct and indirect costs of reducing risk.
- *Fragmented approaches to managing security risk within and across the Federal Government could be addressed by developing Government-wide risk management guidance*.—Some participants agreed that approaches to risk management were fragmented within and across the Federal Government. For example, one participant said that each of the Department of Defense combatant commands has its own perspective on risk. According to this participant, this lack of consistency requires recalculations and adjustments as each command operates without coordinating efforts or approaches. Three participants also said that there is a lack of Government-wide guidance on using risk management prin-

ciples to manage programs. To address this problem, participants said Government-wide guidance should be developed. Two participants suggested that OMB or another Government agency should play a lead role in outlining goals and general principles of risk assessment and getting agencies to implement these principles.

Partnership and Coordination Challenges

Participants agreed that risk management should be viewed as the responsibility of both the public and private sector. They identified challenges related to public-private collaboration:

- *Private sector should be more involved in public risk assessments*.—Participants said that public-private partnerships are important and should be strengthened. One reason partnerships may not be as strong as they could be is that the private sector may not be appropriately involved in the public sector's risk assessments or risk-based decision-making. Participants agreed that the private sector should be involved in developing risk assessments because when these stakeholders are not sufficiently involved they lose faith in Government announcements and requirements related to new risks and threats. To this end, DHS has established coordinating councils for critical infrastructure protection that allow for the involvement of representatives from all levels of Government and the private sector, so that collaboration and information sharing can occur to assess events accurately, formulate risk assessments, and determine appropriate protective measures.
- *Increase the involvement of State and local practitioners and experts*.—Participants observed that intergovernmental partnerships—between Federal, State, local, and tribal governments—are important for effective homeland security risk management. They recommended that more State and local practitioners and experts become involved in applying risk management principles to homeland security.

This concludes my prepared statement. I would be pleased to answer any questions you and the subcommittee Members may have.

APPENDIX I: LIST OF PARTICIPANTS

Moderators

Cathleen A. Berrick: Director, Homeland Security and Justice, Government Accountability Office; Sallyanne Harper: Chief Administrative Officer and Chief Financial Officer, Government Accountability Office; Norman J. Rabkin: Managing Director, Homeland Security and Justice, Government Accountability Office.

Participants

Michael Balboni: Deputy Secretary for Public Safety, State of New York; Esther Baur: Director, Group Communications, Head of Issue Management & Messages, Swiss Re; Baruch Fischhoff: Howard Heinz University Professor, Department of Social and Decision Sciences and Department of Engineering and Public Policy, Carnegie Mellon University; George W. Foresman: President, Highland Risk & Crisis Solutions, Ltd., Former Under Secretary for National Protection and Programs, Former Under Secretary for Preparedness, U.S. Department of Homeland Security; Tina W. Gabbrielli: Director, Office of Risk Management and Analysis, National Protection and Programs Directorate, Department of Homeland Security; James Gilmore: Partner, Kelley Drye & Warren, LLP, Chairman, Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, Governor of Virginia, 1998–2002; Corey D. Gruber: Assistant Deputy Administrator, National Preparedness Directorate, Federal Emergency Management Agency, Department of Homeland Security; Brian Michael Jenkins: Senior Advisor to the President, RAND Corporation; RDML Wayne E. Justice: Rear Admiral, Director of Response Policy, United States Coast Guard; Kenneth L. Knight, Jr.: National Intelligence Officer for Warning, National Intelligence Council, Office of the Director of National Intelligence; Howard Kunreuther: Cecilia Yen Koo Professor, Department of Decision Sciences and Public Policy, Wharton School, University of Pennsylvania, Co-Director, Wharton Risk Management and Decision Processes Center; Peter Lowy: Group Managing Director, Westfield Group; Thomas McCool: Director of the Center for Economics, Government Accountability Office; Susan E. Offutt: Chief Economist, Government Accountability Office; John Paczkowski: Director, Emergency Management and Security, Port Authority of New York and New Jersey; John Piper: Senior Security Consultant, Talisman, LLC; William G. Raisch: Director, International Center for Enterprise Preparedness, New York University; Joseph A. Sabatini: Managing Director, Head of Corporate Operational Risk, JPMorgan Chase; Kenneth H.

Senser: Senior Vice President for Global Security, Aviation and Travel, Wal-Mart Stores, Inc.; Hemant Shah: President and Chief Executive Officer, Risk Management Solutions; Steven L. Stockton: Deputy Director of Civil Works, U.S. Army Corps of Engineers; William F. Vedra, Jr.: Executive Director, Ohio Homeland Security; Detlof von Winterfeldt: Professor, Industrial and Systems Engineering Viterbi School of Engineering, University of Southern California, Professor of Public Policy and Management, School of Policy Planning, Director, Center for Risk and Economic Analysis of Terrorism Events, University of Southern California; Scott T. Weidman: Director, Board on Mathematical Sciences and Their Applications, National Research Council; Henry H. Willis: Policy Researcher, RAND Corporation.

Ms. JACKSON LEE. Thank you very much, Mr. Rabkin.

Thank you both for your testimony.

As I proceed on this question, there are many variables that come to mind when we think about risk. One of the most striking, beyond the horrific tragedy of 9/11 that caused the organization of the Department of Homeland Security and this committee, of which I was one of the early members of the Homeland Security Steering Committee, the organizing committee, was the lack of risk assessment that played into our response during Hurricane Katrina—less so with Hurricane Rita, but certainly the tragedies of what occurred were enhanced or worsened because it seemed as if we had no understanding of how you project risk.

As we watch levees standing or falling in the recent episode of flooding that has created a great deal of tragedy in many parts of the United States, we wonder whether or not we have even improved. So my questions go in the context of reality. That is why we are holding this hearing. Certainly, as all of us have expressed our sympathy to Mr. McInnis, we know that tragedies, incidents can result in loss of life.

Let me start, Secretary Jamison, as I yield myself 5 minutes, to ask you quickly, and your answers please, I have a number of questions. In our letter to Secretary Chertoff dated May 15, 2008, the committee requested quarterly briefings by the Office of Risk Management and Analysis to ensure that it was staying focused on its core mission. Will the Department commit to this request?

Mr. JAMISON. Yes, I would be glad to come up and brief you quarterly or as frequently as you would like to keep you up to speed on our progress.

Ms. JACKSON LEE. We just wanted to get that on the record so we can get that scheduled and to make sure that we have gotten that answer.

The Office of Risk Management and Analysis has asserted to this committee that among its major functions is the construction of a risk lexicon. Many of us think that this is work already done. I assume this is part of a baseline that we are trying to work on. Can you tell us how far along they are on this project, and when can we expect to receive a copy of this particular report?

Mr. JAMISON. We are actually very far along in the process and have been working on it through the risk management working groups within the Department for several months now. We have identified I believe about 80 terms for the lexicon. We expect it to be completed by the end of the summer. Hopefully, that will play a much larger portion role in the broader framework that we are trying to put together in addition to a lexicon, best practices and other strategic frameworks of guidance that needs to be delivered

across the Department and to be implemented down into the national infrastructure protection plan in that framework.

Ms. JACKSON LEE. That would be helpful. I think these quarterly meetings that you will have with us will be important, but we would like to see minutes of the meetings that you are having and try to find out how often these meetings are going on. I have tried to give this hearing a sense of urgency. So how often are these meetings going on in the Department?

Mr. JAMISON. We have meetings at different levels, so we have an integrated framework. We have a steering committee that is at a higher level, an executive level at the under secretary and the assistant secretary level. We also have working group levels that are meeting. I believe the working group levels have met more than 40 times already on trying to work on these strategic issues such as the lexicon, the integrated framework, and RAPID.

Ms. JACKSON LEE. We know the United Kingdom has already organized itself around a national risk assessment for homeland security. It outlines the Nation's risk assessment in Great Britain strategy and framework. Have we done so? Why have we not done so? Or if we haven't done so, why not?

Mr. JAMISON. I think there has been a lot of work that has been done, as you mentioned earlier, in the standup of the Department and all the individual agencies, whether it is TSA or Coast Guard or even the Infrastructure Protection Division.

Ms. JACKSON LEE. But do we have something similar to the one in Great Britain?

Mr. JAMISON. That is what we are working toward.

Ms. JACKSON LEE. We don't have it yet?

Mr. JAMISON. No.

Ms. JACKSON LEE. All right. What about a position for a chief risk officer?

Mr. JAMISON. I think that we have in fact got a chief risk officer as the director of the Risk Management Directorate. The way I have read the report that GAO recommends, you need one person that is in charge of that guidance, and one person that is in charge across DHS in providing that consistency. That is the Risk Management Directorate. It is located within the headquarters and NPDD.

Ms. JACKSON LEE. While I would commend you, Secretary Jamison, and we know that people are hard working, I don't think that office even has a strategy or strategic plan. I would also say that is something that we need to have. But let me continue because I want to ask Mr. Rabkin some questions. I think we are going to make a good start by having these quarterly meetings.

In terms of risk assessment and management, what kinds of communications are being given to State and county and local government which really would have impact on the tragic incident of Goodyear? What kind of directives are coming out for those entities to be conscious of risk and risk assessment and risk management?

Mr. JAMISON. I think there are several ways that we can address that question. I think, as Mr. Rabkin alluded to, the national infrastructure protection framework that we put out to the infrastructure sector and the sector coordinating councils and government co-

ordinating councils is the mechanism by which we communicate with those sectors.

Ms. JACKSON LEE. Government coordinating councils?

Mr. JAMISON. The sector coordinating council process, so for the individual infrastructure sector, for example, the chemical sector has representation from private industry, and communication portals where we provide best practices and provide risk assessments.

Ms. JACKSON LEE. Is that overlapping secretariats? Is that overlapping assistant secretaries that address that within DHS?

Mr. JAMISON. It does overlap because it is critical infrastructure sectors. For instance, TSA has a role in the transportation sectors of critical infrastructure.

Ms. JACKSON LEE. But are you all coordinated? Why don't I just jump to this steering committee concept and ask you how often you all are meeting.

Mr. JAMISON. The working group steering committees are meeting very frequently. We have had strategic executive-level committee meetings as well. We are waiting for the next level of work to be pushed up by the working group level—the lexicon, the framework guidelines—before our next meeting. We have a commitment from Secretary Chertoff to drive this consistency. We also have the commitment from the executive committee of this steering committee to move forward and to get a framework integrated by the end of the year.

Ms. JACKSON LEE. Mr. Secretary, I appreciate it. Glean from my tone a sense of urgency to move forward. We are talking about 2008. I think I heard you clearly that we don't have a chief risk officer, if I am not mistaken. It is long overdue. I am not sure whether we are communicating to local, State and county government—long overdue.

So let me just put on the record that we need these quarterly meetings. We would like to see the work of the team that you have in place, the steering committee, as well as the meetings that are going on. I think time is of the essence and we are urgently in need of trying to understand to protect ourselves. I thank you for answering my questions.

Mr. Rabkin, you mentioned the word "communication." It seemed like that just jumped out at me. It really did because I used the backdrop of Hurricane Katrina. We certainly were not communicating there. That is just one example.

But tell me what progress the Department of Homeland Security made in implementing its risk management framework? In a more important sense, what are the challenges that remain?

Mr. RABKIN. There is progress that has been made. I think the Department has outlined where they want to go. They have communicated that through the national infrastructure protection plan and some of the internal operations that Secretary Jamison has been talking about.

But certainly they have many different components that are all considering risk as they make their own investment decisions, as they make recommendations to the secretary of how much budget they should get and where it should be invested. These kinds of decisions ought to be guided by some common risk principles. I think

that is what this Office of Risk Management and Analysis is planning to do is to get some commonality across.

I understand that they all have individual missions and they should have some flexibility in how they apply the principles, but once the principles are straight and we have some confidence that they are being applied equally, then the secretary can make informed judgments as to which of these various investments get priority and where the next dollar ought to go.

Ms. JACKSON LEE. So what you are saying is this work is crucial in terms of putting these guidelines, these directives in place, to give guidance to the secretary, to give guidance on how we move forward in the Department.

Mr. RABKIN. Absolutely. I think it is only reality that these decisions have been made in the past and some have been more risk-informed than others. They have to be made. Budgets have to be submitted and acted upon.

Ms. JACKSON LEE. Let me ask the obvious question. Does our Government need a national risk assessment? If so, who should lead it? How quickly should we get it?

Mr. RABKIN. If we are talking about homeland security only, then obviously it does. I think it gets it through both the secretary and the Homeland Security Council in the White House that can look across departments and across issues. If we are talking about more than homeland security, if we are talking about risk assessment for all the issues that the Federal Government has to deal with, I think OMB is in a better position to ensure that risk management principles are applied to all the departments, and that the consolidated Federal budget is based on these principles so that decisions about investing in homeland security or any other need—national defense or education or environment—are made based on the same guidelines.

Ms. JACKSON LEE. Since we are starting here in DHS, I think my focus will be getting our shop in order and using the internal mechanisms. Do you think, then, there is great validity in a chief risk officer for DHS?

Mr. RABKIN. I agree with the discussion that took place at our forum, that by identifying someone as a chief risk officer puts credibility and focus on that issue and raises it to the same level as chief information officer, chief management officer, chief human capital officer. That is what the Department deals with all the time, and I think it is appropriate.

Ms. JACKSON LEE. Thank you so very much.

It is my pleasure to yield to the distinguished gentleman from Florida, Mr. Bilirakis, for his questioning.

Mr. BILIRAKIS. Thank you, Madam Chairwoman.

This question is for both panelists. Are there metrics or performance measures that can help determine whether risk-based resource allocation and Federal homeland security programs are in fact actually reducing risks to critical infrastructure and key resources? Can you provide specific examples of how such risk-informed decisionmaking has brought down risk to certain sectors? For both panelists, please.

Mr. JAMISON. I will take a first shot at that. I think that there has been a lot of work across the Department trying to prioritize

risk and to try to incorporate it into the individual areas that we are trying to mitigate risk in, for instance the aviation sector or the maritime sector. There has been a lot of work in trying to prioritize the grant process to make sure we are capturing the threats, vulnerabilities and consequences to effectively give out resources to manage that risk.

We are in the process of trying to get better metrics to determine how that funding and how those resources have driven down and mitigated that risk. The Coast Guard has done some work in that area. FEMA has undertaken that work for their management process. We have a ways to go.

It is a difficult problem to be able to determine how individual pieces of that system of systems of security have an impact that you can bring back and quantifiably measure. But it is definitely the direction that we are going to try to make sure that those investments are having an impact in the State and local communities that we are trying to protect.

Mr. RABKIN. I would like to put a little different twist on it, and perhaps lower your expectations about how much we can quantify risk across the board. When we talk about assessing the risk that is inherent in any of these problem areas or components of homeland security, we are talking about a combination of threat and vulnerability and consequences. So we are talking about how well can we measure what the threat is. Threat, as best I can tell, generates from the intelligence community and is to a certain extent subjective.

Second, we talk about the vulnerabilities of various sectors to attack, either by terrorists or some natural disasters. The vulnerabilities can be better measured. I think we have in the various sectors checklists of things to look for, whether they have closed-circuit surveillance cameras or not, for example; whether the perimeters are secure.

The consequences of any bad event are also quantifiable, but there is a lot of judgment that goes into how far you go and what kind of results you are trying to quantify. If something bad happens, what are the consequences? Well, if a chemical plant is attacked and there is an explosion, there are immediate consequences to the workers and to the immediate community. There are also downwind consequences as the chemicals spread, and you have to try to measure that. There is also the psychological effect of a terrorist attack being successful. That is much more difficult to measure.

Mr. BILIRAKIS. Okay. In your written testimony, Mr. Secretary, you noted that the Department is still working to implement an integrated framework of risk-informed decisionmaking. How far off is DHS from developing a methodology for cross-sector risk analysis? Are you confident that DHS is allocating resources in the most effective manner in the absence of the ability to measure cross-sector risk?

Mr. JAMISON. Well, there are two different efforts that are ongoing that get at the intent of your question, I believe: one within the National Infrastructure Protection Directorate, Bob Stefan's directorate. They are working at a cross-sector methodology across those sectors to aggregate that information and are looking at about five

different methodologies to be able to roll up a more comprehensive risk picture. We anticipate that we will have a lot of that work done by early next year.

There is also the effort across the Department to roll up the risk not only from infrastructure protection, but also from TSA, from the other components into a much broader framework. There has been a lot of work done applying the different program that we have, the well over 120 programs that we have focused on risk mitigation and how they stack up against our priorities.

We are currently going through a methodology called the RAPID process to be able to run some prototypes on different scenarios and to try to give a quantification to how well we are managing risk against those different scenarios. We hope to be able to prototype them in the fall.

Mr. BILIRAKIS. Mr. Rabkin, what are some of the ways that the public and private sectors should apply risk management principles similarly? Are there ways they should manage risk differently? What do you mean when you say that risk communication is the single greatest challenge to using risk management principles?

Mr. RABKIN. I think the participants at our forum focused on risk communication because the decisionmaking process is so inexact as a science. It is an art that is developing. In the absence of solid ways to make these decisions, what really works best is an informed public, sharing of information between people that have it and people that need it.

In the case of the transportation sector, for example, sharing between TSA and the airlines or TSA and railroad operators, passenger rail or freight rail. I think the witnesses on the next panel can talk very well about that kind of interaction between the locals who need to take actions and make investments to take specific actions. Those investments may be funded by DHS. They may be funded locally. To the extent that they have better information and there is more communication that takes place, the more confidence they have that they are making wise investments.

Mr. BILIRAKIS. One more question, Madam Chair? Is that all right? Okay.

During GAO's forum last year on applying risk management in homeland security, participants concluded that the public needs to be educated about acceptable levels of risk and better understanding of the homeland security risks facing our Nation. How did the forum participants propose doing that?

Mr. RABKIN. There were a couple of ideas that were suggested. I don't have them at my fingertips. I can certainly provide them for the record.

Mr. BILIRAKIS. We would appreciate that. Thank you.

Thank you, Madam Chair. I appreciate it.

Ms. JACKSON LEE. The gentleman's time has expired.

Let me thank the witnesses. There being no further questions for our first panel, I thank Mr. Jamison and Mr. Rabkin for appearing before the subcommittee today for this very important hearing.

I am going to request, Mr. Jamison and Mr. Rabkin, that we have a briefing that may come in short order in the month of July, when we have more extensive time of trying to understand where the Department of Homeland Security is in particular, the chief

risk officer's status, and the level of performance in getting to the baseline. We really need to have an understanding both by this committee and the Department of how and what risk means.

Risk means urgency. I frankly believe that we have not captured that as we have moved forward. So I believe that a briefing would be appropriate. So I will look forward to extending an invitation to you, as I thank you for appearing before this committee on this important hearing. The Members of the subcommittee may have additional questions for you, and we ask that you respond to them expeditiously in writing. You are now dismissed.

We now welcome our second panel to take their seats at the witness table.

Let me thank you both very much.

It is my pleasure to welcome the second panel of witnesses. Our first witness, Mr. John Paczkowski, has worked for the Port Authority of New York and New Jersey since 1978, holding a variety of executive-level positions in planning, policy and operations. In September, 2001, he was the assistant director for operations and managed the agency's emergency operations center following the 9/11 attacks on the World Trade Center.

In 2002, he worked in partnership with the Office for Domestic Preparedness to develop and implement a risk assessment program that guided the setting of priorities for a 5-year, $500 million security investment program. This methodology has been applied at over 30 other transportation and port agencies across the country.

Mr. Paczkowski is also a member of the board of directors for the Security Analysis and Risk Management Association. SARMA is a nonprofit professional association serving those responsible for formulizing and managing security risk to systems, structures, operations and information systems from manmade threats. Welcome to you.

Our second witness, Dr. James Carafano, is an expert in defense affairs, military operations and strategy, and homeland security at the Heritage Foundation. Dr. Carafano's research focuses on developing the national security needed to secure the long-term interests of the United States, protecting its citizens, providing for economic growth, and preserving civil liberties.

Dr. Carafano was an assistant professor at the U.S. Military Academy in West Point, New York. He served as director of military studies at the Army's Center of Military History. He has also taught at Mount Saint Mary College in New York and served as a fleet professor in the U.S. Naval War College. He is a visiting professor at the National Defense University and Georgetown University. He is a graduate of West Point, and also has a master's degree and a doctorate from Georgetown University and a master's degree in strategy from the U.S. Army College. You are welcome.

Our third witness is Mr. Raymond McInnis. Mr. McInnis recently lost his wife, Gloria McInnis, on June 11, when a chemical explosion blast occurred in the heat exchange unit of the Goodyear plant in Houston. Gloria had worked at the plant for 31 years as a faithful and dedicated and committed worker.

Mr. McInnis retired from the Goodyear chemical plant in Houston after working there for 38 years as a committed and dedicated and knowledgeable worker, where he rose to the rank of shift fore-

man. Ray and Gloria McInnis were married for 18 years. In his grief, we are very honored and respectful of his presence here today. Welcome, Mr. McInnis.

Our fourth witness is Mr. John Morawetz. Mr. Morawetz has worked for the International Chemical Workers Union Council, which is part of the United Food and Commercial Workers International Union, since 1988. The ICWUC was founded in 1944 and represents more than 20,000 chemical workers in 32 States, including many of them in the State of Texas.

In 1988, Mr. Morawetz was hired as the founding director of the Council Center for Worker Health and Safety Education in Cincinnati, Ohio. In 2005, he was named the director of the union's Health and Safety Department. The center is part of a union consortium made up of six unions. It trains 2,000 participants each year in industrial, hospital and school chemical emergency response and disaster preparedness, and has an extensive worker training and development program which develops rank-and-file workers as educators.

Without objection, the witnesses' full statements will be inserted in the record.

I also want to acknowledge Ms. Sue Davis who has traveled here with Mr. McInnis. Welcome.

I now ask each witness to summarize his statement for 5 minutes, beginning with Mr. Paczkowski. Again, we welcome you. Thank you.

STATEMENT OF JOHN P. PACZKOWSKI, DIRECTOR, EMERGENCY MANAGEMENT AND SECURITY, PORT AUTHORITY OF NEW YORK AND NEW JERSEY

Mr. PACZKOWSKI. Thank you, Madam Chairwoman, Ranking Member Bilirakis and Members of the subcommittee. Thank you for the opportunity to testify here today.

I am John Paczkowski, director of emergency management and security for the Port Authority of New York and New Jersey, and a member of the board of directors of the Security Analysis and Risk Management Association, also known as SARMA. I will be speaking with you from both perspective today.

My organization, the Port Authority of New York and New Jersey, is a bi-State public agency responsible for operating some of the New York region's most significant critical infrastructure, to include its major airports, its largest marine cargo terminals, and its network of interstate tunnels and bridges.

The World Trade Center was our flagship facility and headquarters for over 30 years. Among the nearly 3,000 lives that perished on 9/11, the agency lost 84 of its corporate staff, to include 37 port authority police officers. Having been twice the victim of significant acts of terrorism, and as the operator of transportation facilities that are lucrative terror targets, no other organization is more aware of the importance of homeland security than the port authority.

Following the 9/11 attacks, we conducted a comprehensive series of security audits performed by expert consultants. The results were staggering, with over 20 individual reports, 1,100 recommendations, and potential costs of just over $1 billion. Manage-

ment's reactions were predictable. No. 1, do we really need to do it all? No. 2, what is most important to do first? No. 3, how do we know what will return the greatest security benefit? And No. 4, how will we be able to measure performance?

Beginning in 2002, we partnered with DOJ and later DHS to develop and implement a risk assessment methodology to guide security planning and priorities for our initial 5-year, $500 million security investment program. Since then, we have implemented an ongoing program of security risk management where new assessments are compared against prior results, allowing us to measure the risks as a measure for security program performance.

Unfortunately, as successful as we have been, our results are unique to our agency and not compatible with other efforts on a regional, State or national level, and are therefore of limited value to DHS when assessing overall homeland security risk. Nonetheless, I think our success proves that new approaches to security risk management do work and this should reinforce DHS, the administration and Congress to continue to advance risk management as a national homeland security policy.

Before this body considers what to do next, it is important to note that risk assessment approaches are not being applied in a range of industry sectors at different levels of government, using different methods and with different objectives. As a new field, this is to be expected and to some degree beneficial.

However, we are now at an important crossroads, and in the view of SARMA, stronger and more unified Federal leadership is urgently needed. The focus on homeland security that emerged after 9/11 produced significant new funding for security risk management efforts. Unfortunately, those efforts are not necessarily coordinated or compatible in their approach.

As a result, almost 7 years after 9/11, the Nation has yet to achieve a consistent and well-integrated risk management framework providing decisionmakers at all levels with the ability to intelligently manage homeland security risk. In SARMA's view, this is largely the result of the following factors. Security risk management is an immature discipline that has developed independently and unevenly across the Federal Government and private industry.

There is no national system of governance to guide risk practitioners and ensure collaboration and interoperability in the development or risk management approaches. There is no comprehensive documented body of knowledge on the current state of the discipline from which to implement new security risk management efforts. There is currently no capability to train or certify the knowledge and technical skills of security risk management professionals and bring new entrants into the field.

These factors notwithstanding, SARMA believes there are a few practical steps within existing authorities that can be taken now to remedy the situation. Most significantly, we believe the Federal Government should create a national security risk management program. Under that program, Federal departments and agencies should be required to create a chief security risk officer appropriately positioned and empowered to synchronize, coordinate and monitor all security risk management efforts within their organizations.

A DHS chief security risk officer would harmonize homeland security risk management policies and programs to ensure consistency, compatibility and integration, not only within DHS, but also with State and local governments and the private sector. Moreover, the program would create a risk management governance structure to span the interagency community and bring standardization and rigor to the assessment of security risks, while increasing overall confidence in the process and the decisions that result.

In closing, a more uniform and coordinated approach to security risk management will greatly enhance our Nation's ability to understand and manage the multitude of threats we face now and well into the future. That will lead to improved decisionmaking and more efficient prioritization of resources by not only Congress and the White House, but by the thousands of State and local government and private sector leaders that make up the fabric of our national homeland security effort.

This challenge is beyond the scope of DHS alone, and therefore SARMA encourages the Congress, the White House, Federal departments, State and local governments, and the security profession to join forces and achieve a risk management framework that will provide the Nation with the security it needs at a price it can afford. The members of SARMA stand ready to assist in whatever way we can to help advance this important initiative.

Thank you.

[The statement of Mr. Paczkowski follows:]

PREPARED STATEMENT OF JOHN P. PACZKOWSKI

JUNE 25, 2008

Chairwoman Jackson Lee, Ranking Member Lungren, and Members of the subcommittee, thank you for the opportunity to testify on ways the Federal Government can build on the efforts of the Department of Homeland Security (DHS) and others in applying risk management practices to better secure our Nation. I am John Paczkowski, Director for Emergency Management and Security at The Port Authority of New York & New Jersey and a member of the Board of Directors of the Security Analysis and Risk Management Association.

The assessment and management of risk enables and supports the full spectrum of our national security and homeland security efforts, including decisions about when, where, and how to invest limited human and financial resources. In the face of multiple and diverse threats and hazards, we must accept that security risk—a function of threats, vulnerabilities, and consequences—is a permanent condition, but one that can be better managed through the creation of a well-integrated national framework.

As an emergency management and security professional that has successfully applied risk management practices at an agency level and across multiple transportation sectors, I have experienced the value of using these tools to support homeland security decisionmaking first hand. This experience, as well as my leadership role with SARMA, has provided me with broad exposure to the range of national efforts undertaken in the wake of the 9/11 terror attacks. I will be speaking with you from both perspectives today.

THE PORT AUTHORITY EXPERIENCE

The Port Authority is a bi-State public agency responsible for operating some of the New York/New Jersey region's most significant critical infrastructure. We manage all of the areas major commercial airports (Newark Liberty, John F. Kennedy, LaGuardia, Stewart, and Teterboro); its largest complex of marine cargo terminals (Port Newark and Elizabeth, Howland Hook, and Brooklyn Piers); and its network of interstate tunnels and bridges (the Lincoln and Holland Tunnels; the George Washington, Bayonne, and Goethals Bridges; and the Outerbridge Crossing). The agency also operates the Port Authority Bus Terminal, a major transit hub near the

heart of Times Square and the largest facility of its kind in the world. Our PATH rail transit system is a vital trans-Hudson commuter link and was the target of a serious terror plot foiled by the FBI not long after the London and Madrid metro bombings.

The World Trade Center was our flagship facility and headquarters for over 30 years. We still own that site today and are responsible for its redevelopment. Among the nearly 3,000 lives that perished on 9/11, our agency lost 84 of its corporate staff, to include 37 Port Authority Police Officers. Having been twice the victim of significant acts of terrorism and endured numerous potential threats that thankfully never materialized, and as the owner and operator of vital transportation infrastructure that remain lucrative terror targets, no other organization is more acutely aware of the importance of homeland security than the Port Authority.

Following the 9/11 attacks, the Port Authority conducted a comprehensive series of security audits at all of it facilities. Performed by expert consultants, the results were staggering. Over 20 individual reports, 1,100 recommendations, and a potential cost, by staff's estimate, of just over $1 billion to implement. Moreover, there was no sense of priority among the recommendations. Management's reactions were predictable, and not unlike those of the Congress for the Nation at large: (1) Do we really need to do all of the things recommended?; (2) Assuming we do, if we can't pay for it all, what is most important to address first?; (3) How do we know what types of solutions will return the greatest security benefit given what we have to invest?; and finally, (4) How will we be able to measure the performance of those investments after they have been implemented?

Believing these to be the fundamental questions that would ultimately drive homeland investment going forward, we reached out for assistance to pursue our own security risk management program. Beginning in 2002, we partnered with DOJ, and later DHS, to develop and implement a risk assessment methodology to guide security planning and priorities for our initial 5-year, $500 million security investment program. The methodology permitted the agency to examine an array of potential security threats, assess the criticality of its assets, estimate the potential consequences of successful attacks, and make cross-sector comparisons of risk. Under a DHS technical assistance program, it has since been applied to 36 other transportation agencies across the country.

Following completion of our first assessment in 2002, we have subsequently repeated the process on a 2-year cycle, updating security priorities, plans, and budgets in two successive iterations. In so doing, we have moved the agency from conducting individual risk assessments to implementing an ongoing program of security risk management. As each risk assessment is conducted, the results are compared against the prior one and the change in relative risk is calculated. This comparison shows not only the improvement in the agency's risk profile as the result of new investment but also any changes arising from adjustments to our infrastructure portfolio or the overall threat picture. In this way, we can measure the "buy-down" in risk as a metric for security program performance.

In addition to measuring risk reduction performance, we have worked with DHS consultants to implement a cost-benefit analysis component to the methodology that facilitates comparisons of competing high-cost security alternatives. This tool permits us to evaluate which security improvements or, more importantly, which sets of improvements will provide greatest risk reduction "value" for the money invested and risk reduction potential to be achieved. We recently used this tool with great success in evaluating complex, high-cost alternatives for securing our PATH rail transit system, and will be applying it to the development of our long-range security investment plan going forward. The next evolution of the Port Authority's risk management program will go beyond security risks and examine a range of additional man-made and natural threats in an agency-wide, cross-sector, "all hazards" assessment.

To my knowledge, no other organization at the State and local level has advanced security risk management practice to the degree that we have at the Port Authority. Unfortunately, as successful as we have been, our risk assessment results are unique to our own agency and not compatible with other similar efforts on a regional, State or national level, and are therefore of limited value to DHS when assessing overall homeland security risk. Nonetheless, our success proves that new approaches to security risk management do work, and this fact should reinforce efforts by DHS, the administration, and the Congress to advance risk management as a fundamental element of national homeland security policy.

Before the administration and the Congress consider what to do next, it is important to note that risk assessment approaches are now being applied within a range of industry sectors, at different levels of government, by different agencies, using different methods, and with different objectives. As a new field, this is to be ex-

pected and to some degree necessary. However, we are now at an important crossroads and, in the view of the Security Analysis and Risk Management Association (SARMA), stronger and more unified Federal leadership on this issue is urgently needed to lead and coordinate the numerous duplicative and conflicting efforts in DHS and across the Federal Government.

THE SARMA PERSPECTIVE

SARMA is an all-volunteer, non-profit, professional association serving those responsible for analyzing and managing security risks to individuals, structures, systems, operations, and information. SARMA was founded in April 2006 by career security analysis and risk management professionals dedicated to fostering more effective public/private partnerships to advance consistent, risk-based approaches that provide decisionmakers with measurable results for intelligently reducing security risks. The span of SARMA interest includes terrorism, intelligence collection, cyber crime, and natural hazards. SARMA fosters an open collaborative and non-partisan environment to promote the further development, standardization, and professionalization of the security analysis and risk management discipline for the benefit of the American public, the Nation's security, and the security profession in general.

SARMA's mission is to elevate the practice of security analysis and risk management to a mature, standardized, and consistent discipline among a growing cadre of formally trained and certified professionals, all working together to make the Nation more secure and resilient. SARMA provides a vital link between the Government, the private sector, academia, and individual practitioners. Without this link, homegrown risk methods and theories tend to proliferate, making it even more difficult to coordinate protective efforts between all levels of government or with the private sector.

Over the years, significant resources have been expended by Federal departments and the private sector to implement security risk management processes and methods. However, despite the considerable sums spent to effect improvement, security risk management efforts remained largely unchanged until the terrorist attacks of September 11, 2001. The focus on homeland security that emerged after 9/11 resulted in considerable numbers of new analysts and consumers of security risk information, and also produced significant new funding for security risk management efforts. Nonetheless progress to advance a well-integrated national framework still lags.

DHS, other Federal agencies, academia, and the private sector have used newly available homeland security funding to develop and implement a wide array of new security risk methodologies, which are not necessarily coordinated or compatible in their approach. In addition, various homeland security directives and plans either provide conflicting guidance or remain silent on the security risk assessment methods to be used by Federal agencies, State and local government, and the private sector. As a result, almost 7 years after 9/11, the Nation has yet to achieve a consistent and well-integrated risk management framework providing decisionmakers at all levels with the ability to intelligently manage homeland security risk.

In SARMA's view, this is largely the result of the following factors:

Security risk management is an immature discipline that has developed independently and unevenly across the Federal Government and private industry.

DHS correctly seized on the applicability of security risk management to its mandate of protecting the homeland, but it has not taken steps to ensure the structure, processes, and cadre of qualified risk analysts are in place as necessary to effectively serve the mission. Accordingly, there is still no formal system or framework to standardize technical and professional development or to otherwise build the professional infrastructure required.

There is no national system of governance to guide risk practitioners and ensure collaboration and interoperability in development of risk management approaches.

Absent interagency coordination, an advisory board, and/or a recognized standard-setting body, there is no way to synchronize divergent methods, arbitrate disputes, or resolve crosscutting issues. As a result, risk practitioners often develop new methods rather than adopt or adapt an existing approach. Because the underlying methods currently in use are not based on commonly recognized or compatible standards, the resulting data is often less than useful to others who must then collect similar data using another methodology.

There is no comprehensive, documented body of knowledge on the current state of the discipline from which to implement new security risk management efforts.

There are no common references that practitioners can consult when considering how to best meet their security risk analysis needs. Without such a body of knowledge, there is no way to determine where adequate methods already exist, decide where to focus additional research and development, or ensure existing efforts are not duplicative and wasteful. Moreover, without this collection of knowledge, it will be difficult to train the next generation of security risk analysts and managers in a consistent manner.

The lack of a common professional language for security risk analysis and risk management divides practitioners and makes collaboration difficult.

This "language deficit" serves as a significant impediment to a cooperative approach on security risk analysis and management between the Federal Government, State and local governments, and the private sector. While attempts to set standards within individual Federal departments and agencies have been made, conflict with similar efforts elsewhere only exacerbates the problem. Without a common language for use by practitioners, future progress will remain frustratingly slow.

There is currently no capability to train or certify the knowledge and technical skill of security risk management professionals and bring new entrants into the field.

Given the huge investments being made in homeland security, coupled with the central role of risk management, it would seem logical that training and certification of risk practitioners should be a national requirement. Unfortunately, there is no recognized approach to risk management training in Federal, State, and local government agencies, or in the private sector. Absent this, it is difficult to imagine that risk management will ever be done with the degree of reliability and compatibility that decisionmakers require.

SARMA RECOMMENDATIONS

There are a few practical steps that can be taken within existing authorities, and the support of the Congress, to remedy the current situation and more fully realize the vision of more effectively managing security risks to the American homeland. Accordingly, SARMA recommends that the administration:

Issue a joint National Security Presidential Directive (NSPD) and Homeland Security Presidential Directive (HSPD) to create a "National Security Risk Management Program."

The joint NSPD/HSPD should establish a national program for security risk management, complete with funding for a system of governance over all Federal efforts to implement supporting risk management policies, programs and practices across the interagency community. Such a program would accelerate progress, reduce duplication of effort, and eliminate organizational conflicts and other barriers to implementation.

Require Federal departments and agencies to create a Chief Security Risk Officer (CSRO) appropriately positioned and empowered to synchronize, coordinate, and monitor all security risk management efforts within their organizations.

The Chief Risk Officer (CRO) concept has been in widespread use by the private sector for decades. Implementing such a position within key Federal departments and agencies would elevate the importance of security risk management and end debates over who creates necessary policies and procedures and leads security risk management initiatives at the department and/or agency level. Though we believe that the initial focus of this position should be on coordination of security risk activities, the ultimate goal should be a convergence of all risk management activities within a consolidated CRO portfolio.

Establish a DHS CRSO and harmonize homeland security risk management policies and programs to ensure consistency, and as needed, compatibility and integration, not only within DHS but with State and local governments, and the private sector.

In addition to reconciling and ensuring coordination among all homeland security risk management policies and programs across the Department, the DHS CSRO should identify appropriate DHS agencies and offices to serve as homeland security risk management advocates to State and local governments and the private sector. This would extend the benefits of a common risk management framework to industry and all levels of government as part of a truly integrated and "national" effort.

Create a security risk management governance structure to span the interagency community and bring standardization and rigor to the assessment of security risks, while increasing overall confidence in the process and the decisions that result.

To this end, two essential elements of this structure are recommended:

A Chief Security Risk Officer (CSRO) Council.—The CSRO Council would be officially recognized as the authoritative body for Federal security risk management strategy, policy, and standards. The CSRO Council should include security risk management officials from all agencies with significant homeland security and national security responsibilities. In addition, the CSRO Council would:

- Oversee the implementation of the joint HSPD/NSPD for a National Security Risk Management Program;
- Coordinate and set direction for national security risk management efforts; and
- Analyze and broker resolution of disagreements between Federal departments and agencies over security risk management issues.

An Interagency Security Risk Management Staff.—This interagency staff function would serve as a security risk management Center of Excellence, providing program development support, technical expertise, and training to Federal, State, and local governments, as well as the private sector. The staff would address the shortage of qualified risk methodologists and trainers by centralizing that expertise and making it available to support practitioners in achieving the national goal of a mature, unified, and broadly accepted approach to security risk management. The staff would:

- Provide technical assistance in carrying out security risk assessments and implementing security risk management programs;
- Provide security risk management training, establish minimum training and certification standards, and produce associated training materials; and
- Maintain public/private partnerships to support the use of risk management in the implementation of national security and homeland security policies and strategies.

CONCLUSION

Homeland security efforts since the terrorist attacks of September 11, 2001 have highlighted the difficulty of protecting an almost infinite number of targets with finite human and financial resources. The use of security risk management is the approach correctly chosen by our Nation's leadership to address this enormous challenge. In response, considerable work is underway. Yet, in order to ensure the effectiveness of these efforts, the development and implementation of a well-integrated national framework for security risk management is needed.

The refinement and application of a more uniform and coordinated approach to analyzing security risks will greatly enhance our Nation's ability to understand and manage the multitude of threats we face, now and well into the future. That will then lead to improved decisionmaking and more efficient prioritization of resources by not only Congress and the White House, but by the thousands of State and local government and private sector leaders that make up the fabric of our national homeland security effort.

The creation of a national system of governance and standards for security risk management is beyond the mission and authorities of any one agency. The development of security risk management, as both a process and a profession, is a national priority that cannot be achieved by DHS acting alone. A well-integrated national security risk management framework will require a broad-based partnership with State and local government, private sector industry, academia, and related professional associations. Even with visionary leadership and direction it will not be easy, as the Government Accountability Office and others have noted. Yet such a framework is necessary if we are to protect the people, infrastructure, and economic prosperity of the United States.

SARMA encourages Congress, the White House, Federal departments and agencies, State and local governments, and the security profession to join forces and collaborate to achieve a national security risk management framework that will help provide the Nation with the protection and response capabilities it needs at a price it can afford. The members of the Security Analysis and Risk Management Association stand ready to assist Congress, the administration, and DHS in whatever way we can to help advance this important initiative.

Ms. JACKSON LEE. I thank you for your testimony.

I now recognize Dr. Carafano to summarize his statement for 5 minutes. Dr. Carafano.

STATEMENT OF JAMES JAY CARAFANO, THE HERITAGE FOUNDATION

Mr. CARAFANO. Thank you.

Homeland security, and indeed the functions of all Government, is to enable Americans to live their lives in freedom, safety and prosperity. The key is that it is Government's responsibility to ensure that its measures support all three of those goals equally well. Nowhere is that task more difficult than the issues that we are talking about today, which is managing basically the tools of everyday life that Americans use to go to work, to govern themselves, to take care of their family and their children.

So I would like to offer three brief recommendations. The observations that I am going to offer are based on my 25 years of experience in the Army and issues dealing with national security for over a half-decade working on homeland security issues here in Washington, and being a proud member of a family of first-responders that is filled with nurses and cops and firemen and folks like that.

As a prelude to my comments, I would just like to offer this observation. We live in a great and powerful Nation. That means we live in a Nation with infinite number of vulnerabilities. If you do the math and you want to spend—you pick a number, $25 billion, $30 billion, whatever, taking one vulnerability off the table, you then live in a Nation with infinity-minus-one. It doesn't get you very far.

So you have two options. The one option, which I think everyone here would uniformly agree to, is that we do need a risk-based approach, a rational, not non-political because you can't depoliticize a risk assessment. That is part of the risk management process, but a functional integrated process, as opposed to the opposite which is fundamentally what we generally have now, which is policies are really being driven by constituents and stakeholders that speak out the loudest and get the most attention.

That is a problem because at the end of the day, you just put money where you want, as opposed to where it really needs. It can actually make you less safe. You get less return for your dollar. You actually distract people from doing useful things. You actually undermine the competitiveness of the American economy and the industry, all of which at the end of the day make you less able to withstand a terrorist threat or a natural disaster.

Quite frankly, my grade for the Department of Homeland Security and its ability to move forward on risk assessment and risk management techniques, given the stage it is in its development, is not bad. On the other hand, I would actually grade the Congress much more poorly in its ability to deal with risk management. I think if you look across congressional mandates in border security, container security and mass transit and others, Congress has actually done a very poor job in the sense of trying to use a risk-based approach.

Fundamentally, I think the problem is generally what politicians tend to do, and what we gravitate toward, is focusing on protection. The Government's job is to protect things, as opposed to what I really think the function of Government is, which is to be much more concerned about the resiliency of the Nation, the Nation's ability to move and withstand and deliver goods and services re-

gardless of the political and the economic conditions and different kinds of disasters it might face.

I would argue this is really a product because we really lack a common doctrine and common understanding between Congress and Federal agencies about who does what in risk assessment. I really think that threat assessments and threat reduction are fundamentally a Government's responsibility. It is Government's job to get rid of terrorists. It is Government's job to go after malicious actors.

Criticality or consequence is really a joint responsibility. Government can't do it alone because the private sector has most of the information, most of the knowledge. On the other hand, Government is the only person who can give the broad perspective about what really is a national priority. So that is really a joint function.

I argue that vulnerability assessments, both the assessment of vulnerability and the reduction of vulnerability is really the responsibility of the people who own and use the infrastructure, so it is largely a private sector responsibility. We have really failed to kind of stick to that adherence of responsibilities, so we have really kind of been all over the map.

So very quickly, just three recommendations. One is, Government's role is enormous in the threat reduction area. I think that is primarily where its focus should be. In terms of vulnerability reduction, I think primarily for most infrastructure, the answer from Government is reasonable measures that are largely performance-based that are very similar to the kinds of requirements that we do in public health and safety and environmental.

I think GAO is exactly right. Risk communications and managing expectations are a vitally important job that we really do very poorly. For example, I think it is a very unrealistic expectation to think that Government or the DHS is going to do a risk assessment for the entire country. That means it is going to assess risks and manage the reduction of risks and threat criticality and vulnerability. I think it is unrealistic and unachievable and quixotic.

Third, I think there are some very practical measures that if Government wants to incentivize and move the private sector forward on the vulnerability reduction side, there are some interesting things I think that can be done in terms of liability protections and incentives. I would put the SAFETY Act out as an excellent model of the kind of legislation that could incentivize the private sector to take risk management seriously and to incorporate it into its business practices and adopt realistic and cost-effective means to have a reasonable measure of vulnerability in the infrastructure.

Thank you. I look forward to the questions.

[The statement of Mr. Carafano follows:]

PREPARED STATEMENT OF JAMES JAY CARAFANO

JUNE 24, 2008

RISK AND RESILIENCY: DEVELOPING THE RIGHT HOMELAND SECURITY PUBLIC POLICIES FOR THE POST-BUSH ERA

My name is James Jay Carafano. I am the Assistant Director of the Kathryn and Shelby Cullom Davis Institute for International Studies and a Senior Research Fellow for the Douglas and Sarah Allison Center for Foreign Policy Studies at The Her-

itage Foundation. The views I express in this testimony are my own, and should not be construed as representing any official position of The Heritage Foundation.

Thank you for the opportunity to appear before the committee today to discuss the subject of this hearing "Ensuring our Nation is secure by developing a risk management framework for Homeland Security: How are they measuring risk? Are the risk management principles being followed uniformly?"

My testimony today will focus on the point that risk management is interwoven with the concept of resiliency. The current paradigm of "protecting" infrastructure is unrealistic. We should shift our focus to that of resiliency. Resiliency is the capacity to maintain continuity of activities even in the face of threats, disaster, and adversity. The concept recognizes that we cannot deter all threats or prevent all natural catastrophes. Effective resiliency strategy should:

- *Focus on more than just physical infrastructure*.—Resiliency works with the goal of resilient communities and reflects the geography, culture, economy, politics and other societal factors of the United States.
- *Recognize initiatives must be national in character and international in scope*.—Recognizes that America is part of the global marketplace with a global industrial base.
- *Remain proactive*.—It is a bad idea to wait until catastrophe strikes to discover our resilience, in terms of both humanitarian concerns and Government legitimacy.
- *Manage public expectations*.—Out-of-scale expectations greatly undermine the legitimacy of a national response effort. We must inform the public about what it should reasonably expect in the face of disaster or disruptions. Unreasonable expectations are fueled by both media and political posturing.
- *Define expectations of public-private partnerships*.—Despite the focus on homeland security since 9/11, 5 years after the event the appropriate public and private rolls in dealing with transnational terrorist threats are still poorly understood.
- *Pay greater attention to the development of public and private infrastructure*.—Developing more robust national infrastructure that both enhance the competitiveness and capacity of the United States to withstand catastrophic threats should be a priority.

Resiliency and Risk.—Risk assessments and risk reduction are at the heart of a sound resiliency strategy. Although there are a number of risk assessment methodologies, they all consist of common components.

- *Threat Assessment*.—Examines what our adversary can accomplish and with what degree of lethality or effect.
- *Criticality Assessment*.—Evaluates the effect that will be achieved if the adversary accomplishes his goals. This examines both physical consequences, social and economic disruption and psychological effects. Not all consequences can be prevented. So in order to assist in prioritization, there is a process designed to identify the criticality of various assets: What is the asset's function or mission and how significant is it?
- *Vulnerability Assessment*.—Looks at our vulnerabilities and how they can be mitigated including weaknesses in structures (both physical and cyber) and other systems/processes that could be exploited by a terrorist. It then asks what options there are to reduce the vulnerabilities identified or, if feasible, eliminate them.

Since 9/11, however, the nature of shared public-private responsibility for risk assessment and risk reduction has been poorly understood. Establishing a common appreciation of rolls and responsibilities must be a priority.

- Assessing and reducing transnational terrorist threats is fundamentally a Government responsibility, an inherent obligation derived from the preamble of the Constitution that obligates Government to "provide for the common defense." Threat appreciation and effective counter-terrorism programs that identify, quantify, and reduce threats is not only primarily Government's responsibility, it is arguably the most essential component of risk management. Taking the offensive against terrorist threats is both the most effective and cost-effective means to respond to transnational terrorism.
- Criticality is an activity that must be conducted jointly by the public and private sectors. They equally share responsibility for determining what is most vital to protect the public good. There is no practical alternative to this shared obligation. Most national infrastructure is private hands. The private sector understands best how systems function and impact the economy. On the other hand, only the national Government can offer the national "perspective" of prioritizing needs and obligations in times of national emergency. Thus, criti-

cality can only be determined by sharing information and joint assessments made in trust and confidence between the public and private sectors.

- Assessing vulnerability, determining the best risk mitigation means, managing and providing the resources to reduce vulnerability are largely the responsibility of the entity that owns and operates infrastructure. Most often the consumers and users of the infrastructure and the services they provide bear the fiscal responsibility for implementing measures to reduce vulnerability. These measures should be "reasonable." Vulnerability reduction is an "economy of force" measure, an additional and supplementary line of defense designed to supplement not supplant addressing threats and criticality. Over-emphasis on vulnerability reductions threatens the competitiveness of private sector activity, which in turn could represent a far greater threat to the resiliency of the American economy than any terrorist threat.

Understanding this fundamental division of labor between the public and private sector is fundamental to developing sound public policies.

In order to achieve the goal of "resiliency" as well as to ensure effective risk management, Congress should focus on four initiatives:

1. Promote public-private models for risk management by developing doctrine defining reasonable roles for Government and industry.
2. Encourage bilateral cooperation addressing liability issues.
3. Develop national and international forums for collaboration on resiliency issues.
4. Promote the development of resilient 21st century public infrastructure.

1. Public-private models for risk management.—Public-private models for risk management are essential to the concept of resiliency. A model public-private regime would: (1) Define reasonable roles for both Government and industry through clear performance measures, (2) create transparency and the means to measure performance, and (3) provide legal protections to encourage information sharing and initiative.

Both Government and industry must be given reasonable roles in order to ensure the effectiveness of these models. Understanding, communicating, and reducing threats is primarily a national responsibility, fundamentally a responsibility of Government to ensure public safety and provide for the common defense. It is not the job of the private sector to defeat terrorists. It is the responsibility of the Federal Government to prevent terrorist acts through intelligence gathering, early warning, and domestic counterterrorism.

National Security and Resiliency.—In terms of what is reasonable for the Government, the role of national security instruments should be treated with caution. National security is not about trying to child-proof a country against every potential misfortune. It is the task of protecting people from their mortal enemies—that means other people. These enemies may be from states, trans-states or no states. They may be abroad or homegrown. What they have in common is that they are humans—and that they threaten the Nation by preparing to attack its people for a political purpose.

We should be careful not to dilute the definition of national security to include a plethora of threats or use the proliferation of threats to scope a national resiliency strategy. The Government has many resources to deal with all kinds of problems. Resources, however, are not infinite. National security instruments should be reserved for the critical task of battling those people who plot how to kill citizens, undermine the society and destroy our individual freedoms.

A second reason not to label every "danger du jour" as a national security threat concerns protecting the civil society. In times of peril, the Nation should rely on the Government to provide the common defense—providing the leadership and resolve needed to deal with threats to the Nation. That's why, for example, in the United States the President is vested with the authority to conduct foreign policy and act as commander-in-chief. The U.S. Constitution envisioned an executive who could wield significant power to act decisively in time of war or crisis. That said, the President's national security powers should be reserved only for serious, imminent dangers from America's enemies. Elevating other issues like global warming, pandemics or energy supplies, to the level of national security, only encourages Government to bring the extraordinary powers of the Executive branch to bear on the problem. For the most part, the parts of Government involved in national security should stick to hunting terrorists, thwarting rogue states, and dealing with the other serious enemies who spend their days and nights plotting against the state. In most cases a strategy of resiliency should rely primarily on other instruments.

Criticality as a Shared Activity.—Criticality, on the other hand, has to be a shared activity. In many cases the private sector owns or is responsible for managing both private and public infrastructure that provide the vital goods and services for the

society. Meanwhile, only the national Government has the overall perspective to determine national needs and priorities in the face disasters and catastrophic threats. Thus, they must work together to determine what is truly critical to keep the heart beat of the Nation beating in the face of adversity.

Not all infrastructure should be deemed critical. Indeed, the national designations of "critical" infrastructure and key assets have been detrimental to the effort to prioritize national efforts. The "failure is not an option" mentality with regards to protecting infrastructure has led to an over-zealous approach to "critical" infrastructure. The designation has become increasingly pointless driven by politics and stakeholder interests rather than rational assessments.[1] If everything is critical, nothing is critical.

Vulnerability as a Private Sector Function.—Vulnerability should be largely the responsibility of the entity that owns, manages, and uses the infrastructure. It is largely the private sector's duty to address vulnerability and to take reasonable precautions, in much the same way as society expects it to take reasonable safety and environmental measures.

Resiliency and its role in protecting society actually transcend homeland security and other national security concerns. Resiliency is about building strong, cohesive societies in that can prevail in the face of many challenges whether the malicious acts of terrorists or the heartless whims of Mother Nature.

Indeed, rather than national security instruments, the most common tool to be used in building resiliency is establishing an appropriate legal regime the will allow the private sector and the market place adapt and innovate, to provide a robust, redundant capacity to provided goods services everyday—and especially in times of crisis.

Armed with these assessments and a common sense division of roles and responsibilities, public-private partnerships can set about instituting practical measures that will reduce risk and enhance resiliency.

2. Encourage bilateral cooperation addressing liability issues.—Addressing concerns of liability may be the most vital contribution Government can make to implement a strategy of resiliency. The recent bitter debate in the United States between Congress and the administration over extending immunity against civil suits to telecommunications companies that cooperated with a classified Government surveillance program highlights one of the knotty challenges in promoting public-private cooperation in combating terrorism.[2] Congress can promote private sector participation and alleviate liability concerns by:

- Providing "safe harbors" for sharing critical information;
- Promoting cooperative joint action for public-private partnerships;
- Collaborating with other nations, such as the Technical Cooperation Program (TTCP), an international organization that collaborates in defense scientific and technical information exchange and shared research activities. Promoting liability protection regimes could be the centerpiece of a facilitating global bi-lateral participation in promoting resiliency strategies.[3]

The Safety Act as a Model for Liability Concerns.—A great example of the ability of Government to handle these concerns over liability decisively and with good effect was addressed in the Support Antiterrorism by Fostering Effective Technologies (SAFETY) Act. This Act lowered the liability risks of manufactures that provide products and services for combating terrorism. Passed in 2002, the Act protects the incentive to produce products designated as "Qualified Anti-terrorism Technologies" (QATTs) by the Secretary for Homeland Security. The Department of Homeland Security (DHS) has made a concerted effort to implement the program and a number of companies have availed themselves of the opportunity to obtain SAFETY Act certification.

By addressing liability concerns, Congress intended the SAFETY Act to serve as a critical tool for promoting the creation, proliferation and use of technologies to

---

[1] See, for example, the debate over container security in "Container Security at U.S. Ports: The Heritage Foundation's Research," WebMemo No. 1260, November 27, 2006, at *http://www.heritage.org/Research/HomelandSecurity/wm1260.cfm.*

[2] See, James Jay Carafano, Robert Alt, and Andrew Grossman, "Congress Must Stop Playing Politics with FISA and National Security," Web Memo No. 1791, January 31, 2006, at *http://www.heritage.org/Research/LegalIssues/wm1791.cfm.*

[3] For specific recommendations, see James Jay Carafano, Jonah J. Czerwinski, and Richard Weitz, "Homeland Security Technology, Global Partnerships, and Winning the Long War," Heritage Foundation *Backgrounder* No. 1977, October 5, 2006, at *www.heritage.org/Research/HomelandSecurity/bg1977.cfm.*

fight terrorism.[4] The act provides risk and litigation management protections for businesses that produce QATTs and other providers in the supply and distribution chain. The act included a limitation on liability with regards to third parties claims for losses resulting from an act of terrorism where the technologies were deployed to help prevent or mitigate the danger of a terrorist attack. In turn, the promotion and deployment of new technologies help make the society more resilient in the face of terrorist threats.

3. Develop national and international forums for collaboration on resiliency issues.—Both within the United States and with international partners, the United States should begin to establish regular forums to promote the resiliency concept, share best practices and facilitate joint action.

State-Based Regional Response Network.—Within the United States, these forums could be structured around a regional homeland security structure that promotes voluntary cooperation among States, local communities, and the private sector. The Homeland Security Act of 2002 mandated that DHS set up a regional structure—though the Department did follow through on this mandate. State-based regional programs would focus on ensuring that States are prepared to sustain themselves. Successful regional programs would focus not on Federal structures in each region, but rather on regional emergency management programs and capabilities that are developed, coordinated, and managed by the States. Similar small-scale programs that use a regional model, such as the Emergency Management Assistance Compact (EMAC), have already proven successful. DHS regional offices should be required to strengthen State and local preparedness capabilities; facilitate regional cooperation among Governments, the private sector, and non-Governmental organizations; and plan and exercise with Federal entities that support regional disaster response. Such offices would enable regions to access and integrate their capabilities quickly and improve preparedness and resiliency initiatives.[5]

Internationally, the United States can use both current international institutions and new multi-national and bilateral partnerships to create resiliency forums. For example, the NATO Industrial Advisory Group (NIAG) solicits industry advice on how to promote public-private and transnational cooperation in defense production. This group or other NATO forums might serve as opportunities to discuss resiliency issues.

4. Resiliency's Building Blocks.—Promote the development of resilient 21st century public infrastructure. In the end, public-private partnerships must produce the kind of infrastructure necessary to sustain 21st century societies against 21st century threats. Within the United States much of the national infrastructure is aging and not keeping up with the demands of a growing population. Additionally, for all of the focus on U.S. critical infrastructure, equally vital is the resiliency of the global economy.

What is required is more innovation and experimentation as a means of speeding the development of modern infrastructure. One option to consider is encouraging public-private partnerships (PPP) that invest in public infrastructure. The United States has utilized the PPP model for its public highways and other infrastructure projects. Creating opportunities for governments and private firms to work together on improving the infrastructure should be further explored.

Rather than relying heavily on subsidized public funding of infrastructure, investments should focus on "project-based" financing that shifts the risks and rewards to the private sector. Project-based financing focuses on obtaining stand-alone investment from private investors and could include multiple investors, each with a different level of investment, varying rate of return, and different timelines for realizing those returns. Such strategies not only shift risk to the private sector, but should also lead to improved decisionmaking about needed infrastructure investments.

Resilience is the right strategy.—Resiliency is the right strategy for the United States and its allies in facing the dangers of the 21st century. Congress and the administration can promote this approach both within American communities and across all free nations by means of the initiatives mentioned in my testimony. These initiatives offer a more reasonable and cost-effective means for ensuring the continuity of services and processes, but all for building a more resilient civil society, one prepared to face the future with confidence and surety.

---

[4] U.S. Department of Homeland Security, *Final Rule of the Implementation of the SAFETY Act,* Vol. 71, June 2006, at *http://a257.g.akamaitech.net/7/257/2422/01jan20061800/edocket.access.gpo.gov/2006/06-5223.htm* (March 2008).

[5] See, Jill Rhodes and James Jay Carafano, "State and Regional Responses to Disasters: Solving the 72-Hour Problem," *Backgrounder* No. 1962 (August 21, 2006) *http://www.heritage.org/Research/HomelandSecurity/bg1962.cfm.*

Ms. JACKSON LEE. Mr. Carafano, thank you very much for your statement.

I now recognize and welcome and offer my sympathy to Mr. McInnis, and ask him to summarize his statement for 5 minutes. Mr. McInnis.

STATEMENT OF RAYMOND MCINNIS, PRIVATE CITIZEN, WIDOWER OF VICTIM OF GOODYEAR EXPLOSION

Mr. MCINNIS. Good afternoon, and thank you for inviting me. My name is Raymond McInnis. I live in Houston, Texas. I am a former employee of Goodyear, a retiree of 12 years now and employed for 38 years.

My wife of 18 years, Gloria, has worked at the plant for 31 years—a very knowledgeable person in that plant. She was killed in an explosion at that plant 2 weeks ago today, June 11. It is not easy for me to come here today, but I come here because I want changes made in the workplace. There are so many things that are wrong today that are just sloughed over by OSHA, companies. I have a lot to say. I can't get it done here, believe me. I have heard a lot.

Ms. JACKSON LEE. Mr. McInnis, you can take your time to explain what you are trying to say to us.

Mr. MCINNIS. I just want things to change for her, change the workplace for the people that are working there today and in the future, so that place will be there where people can have a job.

My wife's title at that plant was latex coordinator. She did not work in the part of the plant. It was not her primary duty. Because of the shortage of leadership and supervision, she was there. That was one things she always did. We discussed it. "Why? You don't have to go there. Make them supply supervisors." Well, if they don't have them, somebody has got to do it, and she always went there.

She did not have to be at that place. The thing is, it just lacks supervision and supervisors with training and knowledge. There is a way they go about picking supervisors now that you don't have to know the job. You just take a test and you are a supervisor in a chemical plant. That is what creates these situations.

I would like to go into the story of how this went down and how I found out about my wife's death. On the morning of June 11, I had taken her dog to get groomed, the dog she loved. I went by Goodyear on 225 which I don't ever do, but I saw all the fire trucks and ambulances and what have you, and I figured well, they are having a FEMA drill.

I went on to my home and a friend of my son's, who is a fireman in the city of Houston, made a call to me and asked me how my wife Gloria was. I said, well, I guess all right. He said, well, there was an explosion. I said, well, I will get on the phone, and I will call you back and let you know. I made calls time and time again, and got a recording. The recording was "leave a message." I left messages and called other numbers that I could remember in that plant.

I finally got through to the gatehouse, and one of the security guards told me that she was all right. I asked that question, "Have you seen Gloria?" She said she is all right. So I felt relieved, and

I wait for the 11 o'clock news, local, to find out what really happened. I saw the statement by the plant manager that everything was clear. They had six minor injuries, and everybody was going back to work.

Well, that made me feel much better. I had to call family back and give them all the information—our wife, their daughter, grandmother, mother, and my wife was all right, which made everything all right until that time. Then about 1:45 p.m. that day, I received a call from the same woman that I had talked to at the gatehouse, asking me "Was my wife at home?" I said, "You mean you don't know?" This goes back to the accountability. Where in the heck was it? Nobody is counting. Who is responsible?

Anyhow, I went to the plant. Nobody would tell me. They just passed me from one person to another and led me to the front office. I already had an idea that there had to be something like that, and I ran across one of my former associates at the plant. He told me, "He said, I am sorry, Mac," and I knew then that I had lost my wife.

That was the only notification I had. Nobody would tell me nothing else. All they wanted to do was take me home. I wanted information. I couldn't get any information about anything. All they wanted me to do was go home. So I went. I have had no details of what transpired, what caused the explosion, the people involved. All I know is my wife is gone.

I want changes, the type of changes I want are that the people that work at that plant are trained, supervisors are trained on the job and know the job. Can you imagine in school, every one of us in school, a teacher at some time during your progress, she was there. What was the first thing that woman did? You count your people. You account for them. You want to know where they are at.

This place has no plan like that. They have no supervision to properly set up such a plan for an incident. There is no plan, one man, a foreman with no leaders, and lieutenants in every part of that plant cannot run a proper incident. That is why my wife was not found. Nobody looked. That is why. That is the sad part.

There is a proper way. It has been done, but because of the cuts by the company, to save the dollar, supervision and leadership is gone from that plant. There is no leadership at all. You just can't operate that way.

Where is the script? I am sorry. I just get carried away. I am sorry. I am angry. I want to get back to covering what I came to talk about.

What I found out, and this is the story I found out to go along with that. I found out how they found my wife. After the fire department of Houston was turned away from that plant, because Goodyear gave the all-clear and everybody was accounted for, they had a meeting, calling the supervisor and the people that were involved in this situation. So they were going to have a meeting, a debriefing, and go over what they had. They ordered lunch and somebody happened to say, well, where is Gloria?

Now, that tells you how their accountability system works. They have no idea what is going on in that plant. I am telling you. Please do something about it. I am pleading with you. Check it. I

know every time OSHA comes to that plant, we know about it. Everything is covered up. Everything is prettied up. Everything, for any kind of inspection. This is wrong.

I just want to make sure that everything gets done to help the people of that plant. It is too late, I know, but I want it done for the people there. They need jobs. That is what our economy is about, people working. We are not taking care of them.

I would like at some point for you to ask me questions about how the incident command system should be set up, how it should work. I would be glad to go over that or any other questions you may have for me.

Thank you.

[The statement of Mr. McInnis follows:]

PREPARED STATEMENT OF RAYMOND MCINNIS

JUNE 25, 2008

Good afternoon. My name is Raymond McInnis. I live in Houston and am retired after working 38 years at the Goodyear Chemical Plant in Houston.

My wife of 18 years, Gloria, had worked at the Goodyear plant for more than 31 years before she was killed in an explosion at that plant 2 weeks ago today, June 11, 2008. This is not easy for me but I came here today to talk about what happened to Gloria because I don't want this to happen to anyone else. Neither would Gloria. This may sound corny to you but it's the truth.

Gloria was a Latex Coordinator. She loved her job. But it had gotten harder because of all the cuts at the plant. They didn't have enough supervisors with experience, so Gloria was always willing to help out the team wherever and whenever she could. Her motto was "Somebody's got to do it."

As bad as it is losing a loved one like this, one thing that still haunts me is that after the explosion I was originally told by a Goodyear employee that Gloria was safe. You cannot believe how relieved my family and I were to get that good news. Later, I was shocked when I found out that she was dead and that she had lain there for 7 hours before she was found. How could Goodyear have not known one of their own was missing? Even though I know now that Gloria was killed in the explosion, my first thought was: Would Gloria be alive and at home today if they had realized that she was missing and tried to find her right away?

The explosion occurred at 7:36 a.m. I saw some fire trucks outside the plant at 8 a.m. but because there seemed to be no activity, I assumed it was a drill. A friend of my son's who works in the Houston Fire Department called me later that morning and asked if Gloria was all right. That was the first I had heard of the explosion. I repeatedly called Gloria's office phone but only got her voice mail. I called the Goodyear office with the same result. I called the gatehouse but got no answer. At 10 a.m., I finally reached Jackie at the gatehouse and asked about Gloria. Jackie told me "She's all right."

At that point, I felt relieved. Friends and relatives were calling and I told them Gloria was okay. I watched the TV news around 11 a.m. The plant manager said everyone was okay, only six minor injuries, that the "all clear" was being given. Again, I felt relieved. I kept trying Gloria's office phone and kept getting voice mail. I assumed she'd be out in the plant helping clean up, because "someone had to do it." Gloria's shift was from 6 a.m. to 2 p.m., so I was expecting her home soon.

At 1:45 p.m., Jackie called and asked me "Is Gloria home?" I said, "You mean, you don't know?" That's when I knew. Another woman came on the phone and told me to stay put and they would call me back. I just threw down the phone and rushed to the plant.

The Goodyear plant people kept telling me to go to the office. I didn't want to but finally did. On the way, I ran into a Goodyear employee that I had known when I worked at the plant. He said "I'm so sorry, Mac." That was my official notice from Goodyear. The people in the office kept telling me they were sorry, offering me water, insisting on driving me home. I asked what happened; they said they didn't know. I said I want to see Gloria; they said no, the investigators won't let you. I never spoke with the plant manager, Mr. Lockwood—he talked to the reporters, but he didn't talk to me.

Goodyear drove me home. They later drove Gloria's truck home with her purse.

I ask you ladies and gentlemen of Congress, how can you leave one of your own behind? Why don't you make sure everyone is safe? Who was supposed to count? Who was supposed to report?

When I was a shift foreman, we knew who reported to whom. We knew our responsibilities. We wouldn't have left anyone behind.

Our son is a Marine serving in Iraq. And I want to thank you, Congresswoman Jackson Lee for your help and Congressman Gene Green's help cutting through red tape and getting him home quickly to be with his family at this terrible time. Ask him about leaving anyone behind and he'll tell you a Marine never leaves one of his own behind.

I did not understand why the Houston Fire Department did not go into the plant and search for employees. But my son's firefighter friend explained that the department had considered going in and told Goodyear several times they were willing to go in but Goodyear was adamant that everyone was accounted for. The department weighed that against the danger to their rescue crews and decided it was not worth the risk since Goodyear told them everyone was safe. The fire department left the plant and then had to be called back after Gloria was found by plant workers.

This plant was a disaster ready to happen and its people are not safe today. The plant has done away with its fire department. EMS crews are trained 2 days a year only. The total number of employees has been cut. Contract workers who are unfamiliar with the plant have been hired in their place. Supervisors used to be experienced in all plant operations. Now, you can apply to be a supervisor after working at the plant for 90 days. Equipment is patched up again and again rather than replacing it with new equipment.

Industrial plants are too interested in promoting themselves by giving lip service to safety rather than actually trying to cut the risk of injury to their workers. Worker safety is taking a backseat. Gloria's case shows you that there are failed systems in these plants for accounting for the safety and welfare of the individual workers.

Here is another example. My attorney, Terry Bryant, has represented a number of injured plant workers. He has been told that some subcontractors are so concerned about reporting a good safety record that they confiscate an injured worker's ID card and swipe it at the plant as if the employee were on the job, even though the employee is recuperating at home. They do this just so they can report so-many injury-free work days. You can imagine the situation. If something bad happens at that plant and family members were told their loved ones are unaccounted for. Additionally, first responders could be putting their lives in danger searching for workers who were never there in the first place! Mr. Bryant suggests OSHA should audit these plants to make sure that they have reliable systems in place to know who's really at work and where at any given time and that they have the proper amount of supervision.

Sure, OSHA sets minimum guidelines. But that's all the plants seem to do—the minimum. No one seems to care until someone dies. Then OSHA puts a fine on a company, the company pays it and life for them continues as before. The lives of my family will not continue as before. Do fines really mean anything to these companies? Perhaps if you changed the system to put someone in jail when their greed drives their safety decisions, then they'll pay attention.

The men and women who work at these chemical and petroleum plants do dangerous jobs that are necessary to keep our country functioning. The least we owe them is to do what we reasonably can to ensure that they are safe in view of the risks of their assignments and to make sure that we never again leave one of our own behind.

I was told by one of Gloria's friends that she was with her in the storeroom that morning when they heard about trouble in that part of the plant. She said Gloria told her "I better go over there and see if I can help." Her friend told her she didn't have to do that but my Gloria said her usual, "Someone's got to do it."

Gloria was a wonderful wife, mother, friend and an exceptional employee. If she could have a legacy for her sacrifice, she would want for these plants to be safer for everyone working in them. I thank the Members of the Homeland Security committee for their attention to this problem. I hope a significant improvement will come out of Gloria's death. This is what Gloria would have wanted. God bless you.

I would be pleased to entertain any questions you may have about any statements I have made. Because of the time limit, I could not go into much detail. If you want any more information, you can contact me or my attorney Terry Bryant.

Ms. JACKSON LEE. Mr. McInnis, thank you so very much for your testimony, particularly in this very difficult time in your life. I thank you for being our hero today.

The bells have rung, but Mr. Morawetz, I would like for you to have the opportunity to begin and end your testimony, so we will return and ask questions. Mr. Morawetz will be recognized for 5 minutes. Thank you very much.

STATEMENT OF JOHN S. MORAWETZ, DIRECTOR, HEALTH AND SAFETY, INTERNATIONAL CHEMICAL WORKERS UNION COUNCIL/UFCW

Mr. MORAWETZ. Thank you, Chairman Jackson Lee, Representative Bilirakis, and Members of the subcommittee, for holding this important hearing.

I am here today representing the National Chemical Workers Union Council of the United Food and Commercial Workers Union. I would also like to take a moment to offer my sincere condolences to Mr. McInnis and his family on the loss of his wife.

While we do not represent these workers, we have been active for years in safety issues with hazardous materials and support strong laws to protect both workers and the public. Our members are tragically well aware of these dangers and have a real interest in their facility's safe operation.

In 1971, we represented workers at a Georgia facility that manufactured magnesium trip flares. The facility was evacuated after several small fires broke out, but flares ignited and the plant blew up. Horribly, the evacuation distance was not sufficient and 27 workers were killed. We can and must learn from any event, large or small or from near-misses. This accident served as a valuable lesson in learning what must be done, just as the recent Goodyear explosion hopefully will.

It is far too early to know the full facts and key failure, and most importantly, what the root cause of the explosion was. We believe the explosion took place in a reactor vessel cooled by ammonia that also uses a number of very hazardous and explosive raw materials.

Where the Thiokol explosion led to a better understanding of safe evacuation distances, Goodyear management probably needs to have better training, drills for proper evacuation, vulnerability assessments, and methods for accounting for its entire workforce. These vessels are protected usually from excess pressures by release systems. If an over-pressure situation occurs, a relief valve will relieve the pressure, but often directly into the atmosphere.

I am familiar with this type of failure. In 1990, a BSF facility in Cincinnati where I live exploded. Two workers died and 17 others were seriously injured. I still remember driving down Dana Avenue and seeing the cracked foundations of houses. That explosion was caused by excess pressure that blew a relief valve. The fumes spread around the vessel, found an ignition source, and exploded. Luckily, this release was recognized before the explosion. People were evacuated and a much worse disaster averted.

The Federal Chemical Safety Board is responsible for investigating these incidents and issues excellent reports on their root cause. The CSB visited the Goodyear facility last week, but doesn't have the funds to launch a full investigation. The board also has issued generic CSB reports on nitrogen asphyxiation and chlorine releases. If we are serious about protecting our Nation's chemical industry infrastructure, the question of the proper and improper

use of relief valves should be a subject of a future CSB report and CSB must be fully funded.

Chemical workers know first-hand how a plant works, what chemicals are used, any particular facility's weaknesses, and are responsible for loading and unloading chemical cars. These make chemical workers the first line of defense and explain why we believe employee involvement in the implementation of a plant's chemical security plan is crucial.

Proper and sufficient training is necessary. My union has run training programs and collected data on how much training workers received in the last year in 10 specific areas. Since there is no mandate for refresher training, the vast majority of workers have had none. Effective training needs resources that can be easily understood. New Jersey has written readable chemical fact sheets, that I have provided the committee, for the substances that we believe were involved in the Goodyear explosion.

There are a number of other changes to make chemical facilities safer. First, there must be clear statements and laws to defend workers' jobs if they face disciplinary procedures for reporting any significant security weaknesses. Workers who bravely come forward to protect themselves should not fear losing their jobs when they speak out.

Second, while OSHA standards might be beyond the jurisdiction of this committee, they are a useful model. The process safety management standard mandates that if companies reach a threshold amount of certain substances, there must be operating procedures, process hazard analysis, pre-startup safety reviews, hot work permits, training, and emergency planning. There must be inspections and investigations to make sure that these laws are being followed and enforced. It is fine to have laws and standards, but far too often facilities only act when there is enforcement.

Third, releases that affect thousands of people calls for technology to reduce the risk. These include better-designed containers, reducing quantities, and reinforcing vulnerability sections. Although this committee's mandate is the protection of all facilities from terrorist attacks, I applaud the recognition that we are also discussing natural disasters or so-called accidents.

The chemical workers support the work of this subcommittee to ensure the safety of all and strongly support legislation that has the protections that you have embodied in H.R. 5577. There is no guarantee that any legislation will prevent tragedies like the one at Goodyear, the 27 who died at Thiokol in 1971, the hundreds who died in 1947 in the Texas City freighter explosions, the Bhopal disaster that killed thousands, or future terrorist attacks. But the chemical workers believe stronger laws and enforced regulations will make them less likely.

There is much work to be done to reduce risk and protect workers and communities, and we urge you to act. We look forward to working with this committee to address this crucial problem. Thank you for your time. I am pleased to answer questions.

[The statement of Mr. Morawetz follows:]

PREPARED STATEMENT OF JOHN S. MORAWETZ

JUNE 25, 2008

Thank you Chairwoman Jackson Lee, Ranking Member Lungren, and Members of the subcommittee for holding this important hearing and for the opportunity to testify. I am here today representing the International Chemical Workers Union Council (ICWUC) of the United Food and Commercial Workers Union (UFCW). The ICWUC, which was founded in 1944, represents more than 20,000 chemical workers in 32 States. In 1996, we merged with the UFCW and this mutually beneficial partnership continues to serve our members well.

I would like to take a moment to offer my sincere condolences to Mr. McInnis and his family on the loss of his wife in the Goodyear explosion. While we do not represent the workers at the Goodyear plant in Houston, where the explosion occurred on June 11, we have been active for many years in a variety of health and safety issues which relate to workers in facilities where chemicals are used, especially those with extremely hazardous materials. The ICWUC has supported strong and effective standards and laws to protect both our members and the public.

Unions have a proud history of fighting for the right to a safe workplace and for the basic right for workers to return home after a day on the job as healthy as when they left. From workers who are concerned about their safety and health, to union negotiators seeking health and safety contract language, to unions investigating health hazards or testifying in support of legislation, we are actively involved in making our workplaces safer. It is therefore an honor for me to appear before you to address the safety and health of our members who work in chemical plants.

As to my background, in the early 1980's, I investigated occupational health hazards for the National Institute for Occupational Safety and Health. In the mid-1980's, as the Director of Health and Safety for the Molders Union, I investigated a number of traumatic injuries and deaths and worked to get new standards on the well-documented hazards of confined spaces and failure to lock out equipment. In 1988, I was hired by the Chemical Workers Union as the Director of their Training Center in Cincinnati, Ohio and in 2005, I was asked to also serve as the Director of Health and Safety for the union. I am testifying today in that capacity.

UFCW chemical workers work in many different manufacturing industries including petroleum and coal products, fertilizers, pharmaceuticals, pesticides and other agricultural chemicals in smelters and refineries as well as natural gas distribution and power plants. Our members work with extremely hazardous substances and have a real interest in their facilities safe operation for their own health for their coworkers' health and for their communities' well-being.

The manufacturing of chemical substances involves the handling of highly hazardous materials. The dangers of that work are well known to all workers involved. In a strange irony, the site of one of ICWUC's most tragic loss of lives was a Thiokol facility near Woodbine, Georgia, in 1971. This company started the original manufacturing of synthetic rubber like in the Goodyear plant. The Woodbine plant manufactured magnesium trip flares for the U.S. Army during the Vietnam War.

On February 3, 1971, the Thiokol facility was evacuated after several small fires broke out inside the plant. These fires caused the flares to ignite and the plant was destroyed. Horribly, the evacuation distance was not sufficient and 27 workers were killed when the plant blew up.

This accident served as a valuable tool in learning what must be done to protect workers—just as the recent Goodyear explosion hopefully will. We can and must learn from any event, large or small, or from near-misses. The Thiokol explosion led to a better understanding of the full danger of the materials in that plant and what a safe evacuation distance should be. Clearly, Goodyear management must also look into what needs to be corrected including better trainings and drills for proper evacuation. In addition, given the long delay of knowing what was happening with the workers inside the plant, Goodyear management must improve its methods for accounting for its entire workforce. We have expressed time and time again how important it is to mandate annual training for workers as well as other crucial changes needed to improve workers' safety.

It is far too early to know what the full facts are from the Goodyear explosion—what the key failures were that lead to the explosion and most importantly what the root cause of the explosion was. But after a full analysis, there will likely be a root cause and that is where we can learn our most important lessons. From what little we know, the explosion took place in a reactor vessel, which was cooled by ammonia, a very dangerous substance by itself. In addition, the reactor handles a number of very hazardous and explosive chemicals. The dangers of these chemicals are

also very significant and well known. After the explosion, a number of workers were hospitalized due to exposure to ammonia.

In this synthetic rubber operation, as in others, the pressure vessels such as reactors, storage tanks and process vessels are protected from excess pressures by pressure relief systems. These systems consist of one or more relief valves that are preset to a certain level if an over-pressure situation occurs the valve will relieve the pressure until it again drops to the regulated amount. The problem with the relief systems at many facilities is that they relieve directly into the atmosphere. In the 1970's and 1980's, many States passed legislation that required the relief systems to relieve into an internal closed system. This system can be a recovery system, flare stack or some other way of not having the explosive or flammable vapors relieve to the atmosphere. Most of the legislation provided that the companies were not required to install the closed systems if it was not feasible. Companies could be exempted if they thought changing the system would be too expensive.

I am very familiar with this type of failure. On July 19, 1990, a BASF facility in Cincinnati, where I live and a facility that my neighbor retired from, exploded. Two workers died, 17 others were seriously injured and there was extensive damage to houses in the neighborhood. I still remember driving down Dana Avenue and seeing the cracked foundations of people's houses. The analysis of that explosion pointed to a reactor vessel that over pressurized and blew a relief valve. These valves were designed historically to vent steam to the atmosphere, a significant heat hazard but not explosive. The releases we are talking about today however are very explosive substances. In Cincinnati, the fumes spread around the vessel, found an ignition source and exploded. Luckily, the hazard of the over-pressurized vessel was recognized, people were evacuated and a much worse disaster was averted. But again, there are lessons to learn from this explosion.

Many, if not the majority, of these chemical facilities never installed the closed systems. The danger associated with this technology is that if there is a terrorist event that results in a fire and subsequent evacuation, reactions will go wild. When reactors build excessive pressure, their relief systems will vent to the atmosphere. Since many of these chemicals are heavier than air, they will drift to the ground and find an ignition source. As a result, more explosions will take place.

Prior to the Goodyear plant opening in Houston, there was another Goodyear facility in Akron, Ohio that produced the same product. One of the main reasons for moving the production was the Houston plant had much larger reactors that could produce larger quantities of the product. Yet, the Akron facility, unlike the Houston facility, had relief systems that vented to a closed system such as a flare stack or recovery system. It is reported that the Texas facility's largest tank could release up to 18,500 pounds of ammonia in a single event endangering 35,000 people at a distance of up to 1.7 miles. The largest single event of 1,3-Butadiene, a powerful carcinogen and reproductive hazard, could release up to 1.1 million pounds endangering 4,300 people. There is also a chronic risk to the community with releases of these chemicals.

Clearly, this type of release that can affect thousands of people calls for safer technologies in these plants including chemical substitution and safer process systems. While the Houston plant has relief systems, it is likely to be an atmospheric relief system. Closed relief systems can mitigate an accidental event, terrorist activity or natural disaster. This Goodyear facility serves as a strong reminder of why vulnerability assessments of these facilities are required; why workers should be involved in those assessments; why annual drills should take place; and why workers need to be better trained.

The Chemical Safety Board (CSB) is the Federal agency which is responsible for investigating incidents like that at the Goodyear facility. In the past, the CSB has issued excellent reports that get to the root cause of an incident and then publish recommendations for preventing future similar events. The CSB did in fact visit the Goodyear facility in Houston recently but did not have the funds to launch a full investigation. In Cincinnati this last weekend, a worker died from what looks like overexposure to hydrogen sulfide that was released when some chemicals reacted in a wastewater treatment facility. CSB had a team at the scene but does not have the funds to fully investigate.

These national tragedies need to be fully investigated, the causes determined, reports written and then the results must be widely distributed. The CSB must have the resources to do its job. In addition, the Board must be able to research all individual releases, evaluate the generic problems and then offer solutions. There are CSB reports on nitrogen asphyxiation, chlorine release from large containers and combustible dust. If we are serious about protecting our Nation's chemical industry infrastructure, the question of the proper and improper use of relief valves should be a subject of a future CSB report.

Reviewing what happened and learning from all accidents including the Goodyear explosion is crucial to protecting chemical workers. Besides accidents that can injure and kill workers, chemical plants can also become the targets for terrorists' attacks. Whether it is from a terrorist attack, accidents, or from natural disasters, the result threatens the safety of workers and surrounding communities. This vulnerability is well documented and has resulted in many important legislative discussions.

Currently, the Department of Homeland Security (DHS) has addressed a National Risk Management Framework to protect our critical infrastructure and key national resources. This DHS Risk Management Framework identifies a number of key steps, one of which is "Implementing Protective Programs." Much of what the current CFATS regulations require in collecting Top Screen information and assigning facilities to tiers remains in place. What will be different is the implementation of these protective programs as well as what should be included in the programs. Crafting well-thought-out legislation and regulations is no easy task and we appreciate the subcommittee's efforts to draft legislation that will address the problems. As you know, the current DHS regulations expire in October, 2009. It is important that chemical workers and their management have as much time as possible to plan for any final rule. It is critical that we have the time to address our concerns and hope you will move legislation that will help us resolve these concerns.

In order to improve the safety of chemical plants, it is crucial that we also concentrate on worker involvement in security plans, effective training requirements, strong whistleblower protection, strong OSHA standards and use of methods to reduce the consequences of a catastrophic release.

A key element in enhancing chemical plant security is worker involvement and participation. Chemical workers know first-hand how a plant works, what chemicals are used, how those chemicals react to one another and any particular facilities' weaknesses. We know the exact location of hazardous materials and we know if our training is really effective. We also know if backup systems will work when the power goes out. We are responsible for off-loading and loading chemical railway cars and transferring them around the plants. It has long been known that workers have direct and current knowledge and experience of plant operations that is invaluable in solving site-specific problems. All these responsibilities make chemical workers the first line of defense and explain why we believe employee involvement in the drafting and implementation of a plant's chemical security plan is crucial. It is a vital national resource that workers' expertise—the same expertise that operates these plants everyday—be utilized. All plants should take heed of its workers' expertise and concerns—prior to an explosion occurring. Including chemical workers in this process will enhance facility security and protection.

Proper and sufficient training is also crucial in protecting workers. My union has run training programs and collected data on how much training our members received in the last 12 months in ten specific areas. Since the primary OSHA training mandate, the Hazard Communication Standard, only requires training on initial assignment, the vast majority of workers have had no recent training in Engineering Controls, Air Monitoring, Decontamination, Toxic Effects, Emergency Response Procedures, OSHA Regulations, or Hazard Recognition (the actual percentage ranges from 69 to 89 percent with no training). About half of these workers did not receive ANY training in ANY of these areas. Although I do not know what kind of training the workers at Goodyear had, I do know that there is really no such thing as too much training. The Government and companies must increase the amount and type of training to all workers inside these plants.

Let me add that to conduct effective training you need resources that can be easily understood. It is no coincidence that New Jersey, a State that has taken a strong interest in the security of their chemical plants, has devoted a considerable amount of time and effort over the last 30 years to write readable and valuable resources on these key issues. I have provided some of those fact sheets to the Chairwoman on substances we believe were involved in the Goodyear explosion including ammonia, 1,3-Butadiene and styrene.

Another key element of improving the safety in plants must include a clear statement and defense of workers' jobs if they face disciplinary procedures for reporting any significant security weaknesses at their facility. Fear is a fact of life at all too many workplaces and jeopardizing one's job by blowing the whistle is a risky thing to do. Defending members' jobs is regrettably all too common a task unions are forced to do. Workers, who bravely come forward to protect themselves, their coworkers, and communities around the plant, should not fear losing their jobs when they speak out. Whistleblower protection is vital in assuring the free exchange of ideas, improves security and ensures that effective measures are actually implemented. Workers must have the ability to come forth and communicate program deficiencies without fear of retribution.

Occupational Safety and Health Act (OSHA) standards are beyond the jurisdiction of this subcommittee but they serve as a useful model and one that needs to be considered. Many, but by no means all, hazardous chemicals are already part of the standards that have improved our facilities. There are also broad standards that apply to many workplaces that improve the ability to investigate health hazards and make further improvements. We have a relatively easy time getting Material Safety Data Sheets (MSDS) on substances our members are exposed to, thanks to OSHA's Hazard Communication Standard. I worked in a wire and cable factory before this law went into affect and we did NOT know the contents of containers or what the chemicals could do to us. This Communication Standard changed that and is an invaluable tool in health investigations. Recently, I left a message for a company's health and safety representative about our members getting sick working around a new product line. Within 2 days, I received the MSDS for the substances and an industrial hygiene report on a sampling that was done—all without ever talking to this staff person.

It is also possible that lists of chemicals and threshold amounts from one standard can dovetail with another. One standard that probably applies at Goodyear is the Process Safety Management Standard (PSM), 29 CFR 1910.119. If companies reach a threshold amount of these substances, this standard mandates investigation of their processes, clear operating procedures, regular inspections, process hazard analysis, procedures for contractors, pre-startup safety reviews, procedures for mechanical integrity, hot work permits, mandatory training, incident investigations, emergency planning, compliance audits and written procedures for any process changes. Ammonia is covered by this standard but from what I can tell, the raw materials, 1,3-Butadiene and styrene are not.

I do not know the PSM procedures in place at this Goodyear facility but nationally there needs to be inspections and investigations at chemical plants to make sure that this law is being followed and enforced. It is all well and good to have general recommendations and laws but far too often facilities only take note when a law is actually enforced. Unfortunately, laws mean little if everyone knows that they will never be enforced. Even in the best of our facilities there is always room for improvement. One facility that comes to my mind is actually trying to implement the right procedures but after careful review, I realized that all the drills were taking place on the first shift. This is probably because that is when the salaried employees work. Yet, this facility has three shifts and operates continuously. At the end of the day, only a fraction of the workers are being drilled for these types of events.

There are many steps and measures that could and should be taken to improve chemical plant safety and security. Substituting less dangerous formulations, different size and better designed containers, or various engineering steps, can minimize the consequences of an accident or attack at a chemical plant. This safer technology can significantly reduce the risk of a catastrophic release of chemicals from intentional attacks or unintentional disasters. Although safer processes may not be feasible in all circumstances, either technologically or economically, safer solvents or formulations should be substituted for more dangerous ones. The quantities can be reduced, stronger containers can be used, vulnerable sections can be reinforced and maintenance schedules must be reviewed.

It is invaluable to devote time and funds to develop technologies and practices to decrease threats, vulnerabilities, and consequences of any event. I recently toured a facility, located just outside a major urban area, which utilizes a significant amount of chlorine in its operation. In discussing the potential danger with management and the union representatives, they explained that they had analyzed ways to minimize the risk including using smaller containers. They concluded, rightly I think, that given the volume they use, that smaller containers would have to be changed out so frequently that the risk of releases would be that much greater by using the smaller containers. When I suggested that perhaps these large tank cars could be designed better to minimize the consequences of any failure, they agreed that might be a partial solution. Clearly, we must put on our thinking caps and consider every possibility to make these facilities safer.

Although this subcommittee's mandate is the protection of our facilities from terrorist attack, I applaud the recognition that the measures that you are discussing will protect us not only from a terrorist attack but will also minimize a hazardous release from a natural disaster or so called "accidents." The dangers we face in a chemical release come from a variety of directions, but these changes as outlined in my testimony will mitigate the consequences and risks of a release regardless of the cause of that release.

Homeland Security Presidential Directive No. 8 on National Preparedness stated that we must "strengthen the preparedness of the United States to prevent and re-

spond to threatened or actual domestic terrorist attacks, major disasters, and other emergencies by requiring a national domestic all-hazards preparedness goal." Worksite measures and improvements will result in changes that go beyond a possible terrorist attack and will address a wider range of hazards as stated in this Directive. They will minimize the threat of not only attacks, but catastrophic events and releases which are a reality that chemical workers and the public living around plants experience frequently.

The International Chemical Workers Union Council supports the work of this subcommittee to ensure the safety of our chemical workers, the communities around the facilities and all Americans. We strongly support legislation that has the protections embodied in H.R. 5577. There is no guarantee that any legislation will prevent tragedies like the one at Goodyear, the BP explosion in 2005 where 15 contractors died, the 27 who died at Thiokol in 1971, the hundreds who died in the 1947 Texas City freighter fire and explosions, the Bhopal disaster that killed thousands, or a terrorist attack but the ICWUC believes it is necessary to make these changes in law and regulations. There is much work to be done to reduce risk and protect workers and communities. You have heard today of the real risks and you have the opportunity to take significant steps forward. On behalf of the ICWUC, I urge you to act now to protect America—to protect all workers and their families—by reducing the consequences of any release, be it intentional or unintentional.

The ICWUC looks forward to working with every Member of this subcommittee and the House of Representatives to address this crucial problem. Again, I thank you for your time and would be pleased to answer any questions that you may have.

Ms. JACKSON LEE. Mr. Morawetz, I thank you for your testimony.

I thank all the witnesses for their testimony. As you have been hearing a number of bells, I hope that by being here in the Capitol you realize that Members have been called to vote. I am going to now yield myself 5 minutes for questioning. I am going to start with Mr. McInnis, and then we will recess probably midway in the middle of the questions, Mr. McInnis. We ask the witnesses to in essence, Mr. Carafano, stand down. We will come back as quickly as possible to proceed with our questioning.

This is an enormously important hearing, and we thank you gentlemen for your testimony. But I think, Mr. McInnis, you have crafted the overall and broad theme of this hearing. That is why it is so important for you and the other witnesses to be here. It is risk assessment and it is the ability to respond to that risk.

This is an incident that occurred, and at this point of the investigation, we don't know, if you will, the genesis. We will not define this as a terrorist act. We make it very plain. But this committee has the responsibility of risk assessment for the Department of Homeland Security. It covers a number of ranges of parameters that may occur. We must protect against what might be.

So you made a very important point, and I want to go back to that. That is the de facto search. That is the lunch meeting where lunch is ordered, meeting is gathered, and then a de facto search occurs by some humble soul asking, "Where is Gloria?"

I will ask Mr. Paczkowski the same question, having been present during 9/11. One of the major issues was the logistics of search and accounting for persons.

So Mr. McInnis, would you please tell us I think what you wanted to, the line of command, or what you thought of in a situation of a de facto search, where a meeting was called, lunch was ordered, and all of a sudden someone said, "Where is Gloria?"

Mr. MCINNIS. Yes. There is a plan for that and an incident command set up. That is why I say they are short of personnel. You have a plan, I think all these plants have it, and all these people

know. You have a supervisor in each area who has a responsibility for his people to keep count in an evacuation or any incident.

Because of the lack of supervision to do this and lead, they don't have that. It is just everybody run for themselves.

Ms. JACKSON LEE. So there is no one, you are saying, that paused for a moment and counted one, two, three, four, five, six, seven, eight, and knew that all persons were out.

Mr. MCINNIS. It is obvious they didn't, ma'am. One was still missing for 7 hours and they didn't know it. I hate to say it that way, but no, it doesn't work. They have no idea what they are doing. They haven't set it up. If they did, it would have been fine, but no. How do you think everybody felt in the family when we find out they were going to have lunch and go over what happened, and somebody says, "Where is Gloria?" You know? They don't know. They don't have any idea what is going on out there.

I am sorry. I got expounded on that, and I forgot the second half of what you asked me.

Ms. JACKSON LEE. I will ask that question when I return, but what I was asking is, do you know if there is a plan where there is a chain of command that would have someone be responsible for all the persons and it is a known plan?

Mr. MCINNIS. There was when I was there 12 years ago. They have cut the force so much, I don't know what the plan is, or do they have it in writing. I am sure they have it in writing, but can they implement it properly with the people they have? I am sure they have a plan.

Ms. JACKSON LEE. Let me, Mr. McInnis, we are now going to declare that the hearing is in recess. I have to go vote, along with other Members who have been in markup. We will return in short order.

The hearing is now recessed to be convened in a very short moment.

[Recess.]

Ms. JACKSON LEE. I call this meeting back to order.

As we recessed, we were questioning Mr. McInnis. I am going to allow Mr. McInnis to give us any thoughts that he may desire, and then yield to the distinguished acting Ranking Member, who had a meeting and who is now here, for his 5 minutes.

I do want everyone to be aware of the enormous sacrifice that Mr. McInnis is making. I know that other witnesses certainly respect that. We respect their presence here. I frankly want to place on the record, Mr. McInnis, that you are doing a remarkable job, and we thank you because you are making a sacrifice. We appreciate it.

So right now, I am going to yield to you. I don't want to gavel, but to allow you to finish your thought that you may have had as I was leaving. Then I am going to yield to Mr. Bilirakis.

Mr. MCINNIS. Thank you very much.

First off, I want to make a comment. The people at Goodyear, the employees who work there, these are not the guilty people. I think when I rant and rave, I may have said things, but it is not the people that work at that plant. It is the company that developed by the hierarchy of Goodyear itself to set this kind of operation in motion. They have to follow the procedures that Goodyear sets for

them. So I just want to make that clear. The people and employees of Goodyear itself in that plant are not guilty of anything. It is the culture and the set-up by the hierarchy of Goodyear itself that created that situation.

So thank you.

Ms. JACKSON LEE. Let me quickly ask Mr. Paczkowski in my time remaining, how important, upon reflection, is the knowledge and the acceptance of the responsibility of establishing a risk assessment on any number of infrastructures we have? What is the level of importance of having a logistical plan that provides for accountability or accounting of all those that would be under your command?

Mr. PACZKOWSKI. Well, Madam Chairwoman, I think that accountability of personnel, both before and after an incident, is extremely important. I had the unfortunate experience of living through both the 1993 bombing of the World Trade Center and the 2001, and I can tell you that one of the things we did in the emergency operations center was not only accountability of Port Authority personnel, but also everyone else who was either working in or visiting the World Trade Center complex on 9/11.

Of course, the tremendous amount of effort that went into accountability right after that event, we have established those as standard operating procedures in our emergency plans. The change of command that exists even pre-event doesn't stop post- of that, once the evacuation begins. Our supervisors are trained to make sure that they account for those persons. In every evacuation drill at our facilities, we practice personnel accountability, so it is extremely important in terms of the planning that we do.

Ms. JACKSON LEE. Let me thank you. We will have a second round.

I now recognize the distinguished gentleman from Florida for 5 minutes.

Mr. BILIRAKIS. Thank you, Madam Chairwoman. I appreciate it.

Again, Mr. McInnis, thank you for appearing. I, too, would like to give you some time if you wanted to add anything else that you haven't already stated.

Mr. MCINNIS. I would like to take this opportunity to the whole committee, but I also want to extend my thanks to Mr. Gene Green and Sheila Jackson Lee for helping me get my son back in a difficult situation from Iraq. We struggled with that. I had a lot of problems, and the kid sat on a tarmac for 3 days not being able to get home. Through your efforts, he got home very quick, and I appreciate you all doing that very much. You don't know how much it means to the family. Thank you both, and the committee.

Mr. BILIRAKIS. Mr. Carafano, you argue that resiliency is the right strategy for homeland security. Do you not believe that the Federal Government currently considers resiliency as part of risk management? How do you believe the Federal Government should focus on resiliency?

Mr. CARAFANO. I think the problem is we never start—we used the term "risk management" from the beginning, but we also talked about protecting critical infrastructure. What has overwhelmingly kind of driven the train is really this notion of protecting critical infrastructure.

Well, there are two problems with that. One is, protection is a strategy. Again, when you live in a society with an infinite number of vulnerabilities, it is much more cost-effective to reduce threats than it is to try to eliminate vulnerabilities. The second notion is, the term "critical" quickly became politicized. Pretty soon, everybody wanted to be "critical." So we have an overwhelming abundance of critical infrastructure now.

So in a sense what we have is a lack of focus. Again, I think it is largely not driven by DHS, which I think if left to their own devices would want to not just impose risk management philosophies, but to focus the resources on what is truly the responsibility of the Department, which is dealing with transnational terrorist threats and coordinating national response in the face of catastrophic disasters.

Again, I think a big challenge here is to Congress. If you think about it, if Congress wants to be a player in risk management, it has to do business differently. It has Congressional Research Service. It can say this is the state of the debate. It has the CBO, and that can tell you this is what it is going to cost. And it has GAO, which can tell you this is how effective the processes are.

What they don't really have is they don't have an investigative arm or an assessment arm themselves that assesses outcomes, that really looks at whether this makes sense. This is traditionally what is called operational research, which just doesn't look at the process itself, but looks at the outcome this produces.

So once Congress has some kind of mechanism similar to, for example what the Government relies on, in terms of FFRDCs, federally funded research and development centers, like RAND and MITRE and these kinds of corporations, but until they have some kind of in-house capability to do risk assessments to both be a check on Government, and to do assessments of what is reasonable, Congress is just kind of taking a stab at what they think kind of sounds intuitively right. I think the record so far shows that Congress doesn't really get it very right very often.

Mr. BILIRAKIS. Okay.

Mr. Paczkowski, do you believe there should be a national standard for risk methodology that could be used at both the public and private levels? Who do you believe should be responsible for developing such a standard? Has any group in the private or academic arena attempted to develop such a standard?

Mr. PACZKOWSKI. Well, I think there is no one standard. I think that risk management is both a process and a profession. We are advancing improvements in process all the time, but we are not developing the professional infrastructure to make that happen. A piece of that is standardizing terminology, standardizing process, much in the same way like other professional disciplines would do in engineering or accounting.

Where it should reside in the Federal Government, I am not really sure, except it should be in a position where it could influence the development of risk management across the interagency community, wherever that is best placed. Organizations like OMB come to mind, but I am not necessarily certain whether that is the right place or not.

Certainly, I believe that risk management in the way we have talked about it is larger than the Department of Homeland Security alone, and it requires a kind of interagency perspective that I am not sure the Department alone can provide.

Mr. BILIRAKIS. Thank you, Madam Chairwoman.

Ms. JACKSON LEE. I thank the gentleman.

We will now begin a second round.

Let me ask Mr. Morawetz, your testimony was very moving. As you well know, we have authored in this committee the chemical security bill, H.R. 5577, that really is applicable to any incident that occurs in the course of a chemical plant's responsibility to its employees and also to the issues of safety and security.

For example, the bill, H.R. 5577, which we are looking to move as quickly as we can in light of the dual jurisdiction that occurs, has a provision, the role of employees in vulnerability assessments and site security plans, which means these are overlapping responsibilities, that if you secure a plant for the potential of a security risk, it also I think spills over, if you will, into securing the plant for it to be safe.

You have mentioned several incidents, which I would like you to go forward and use, the present state of affairs as possibly contributing to companies not having risk assessment plans, processes for accounting for employees, certainly safe handling of chemicals, which we found lacking.

If you would answer that question, then would you explore the point you made about the Chemical Safety Board not having enough funds to investigate, which I frankly believe is an appalling, outrageous posture and position to have heard in a hearing room in the U.S. Congress of a committee that deals with homeland security.

So if you would, Mr. Morawetz, approach those two questions for us.

Mr. MORAWETZ. Let me start with the second one. From what I know, and I am not an expert on the Chemical Safety Board, is they are a relatively new Federal agency. They are modeled after the FAA. When there is an accident, they go investigate it. I think that that is a good role model and one that is deserving, but it is interesting that it is recent. There wasn't such a body before 10 years ago.

They are relatively small. They have a budget of I believe about $9 million. They have a small staff of 40 employees. As much as I would like them to investigate this incident, I hope it is not at the sacrifice of another town in another part of the country which can't get an investigation. For instance, in my written testimony, I think it was there, in Cincinnati last weekend we had an employee die in a wastewater treatment facility from hydrogen sulfide exposure. I believe again that the Chemical Safety Board was going to go, but I am not sure whether they can investigate it.

That dovetails for me into more these generic problems. It is not the only wastewater treatment facility. Goodyear in Houston isn't the only synthetic rubber facility. CSB has done these generic reports which I think are very valuable. The recommendations they make can apply to a number of facilities, and as I said, the relief valve. So that is what I know about the Chemical Safety Board.

Ms. JACKSON LEE. It is funded, I think for the record, it is a federally funded entity?

Mr. MORAWETZ. Yes. It is a Federal agency.

Ms. JACKSON LEE. So when you speak of funding, I just want to make sure the record is clear, you are suggesting that there has been a short-changing or a difficulty in funding the agency.

Mr. MORAWETZ. I don't think they have enough funds. I would defer to other people. You probably know much more about the Federal budget and how that works. But it is relatively small and has a relatively small amount of a budget.

Ms. JACKSON LEE. Well, you can feel perfectly free to suggest, if that is what you believe, that there is not enough funding. Yes, we do have to make budget decisions, but we also have to make risk assessment decisions, and we have to prioritize decisions. So is your testimony that you would believe that there needs to be more funding for the Chemical Safety Board?

Mr. MORAWETZ. Yes, that is correct.

Ms. JACKSON LEE. And that there is a greater need than what is imagined with a budget that may be $9 million, maybe a little bit more, and with 40 employees?

Mr. MORAWETZ. Yes, that is correct.

Ms. JACKSON LEE. You may continue.

Mr. MORAWETZ. The other one, you raised some points about homeland security, H.R. 5577, which I am familiar with, but also what comes to mind is the Goodyear situation. It is very interesting having this hearing because when I look at risk management in the context of this committee, it is one answer. When I look at risk management as I do for these facilities, all of them, what comes to mind to me, and it is part of my testimony, is that, wait, what we really need is enforcement of the standards that are in existence.

If those standards were enforced better, I think there would be a bottom level that would be more protective for a lot of facilities, that then we would have to undoubtedly do more on for terrorist threats and other threats. But without that bottom line, that basic level of protection, we are in a very difficult situation. I don't want to just think about the terrorist threat, and then those facilities for instance with the current CFAS rules that don't have the threshold, fall through.

Ms. JACKSON LEE. Do you think that threshold is the responsibility of the Federal Government, whether it be the Department of Homeland Security or another agency, to establish a baseline of risk or a baseline of what is necessary to protect critical infrastructure that may be subject to incidents like Goodyear and what you have mentioned, and obviously, unfortunately some untoward action that may be premeditated?

Mr. MORAWETZ. In general, I support the CFAS regulations, that idea of a threshold amount. I do equally support the idea of the process safety management threshold amounts. What also comes to mind are other standards like hazard communications in my field that do not have a threshold amount. If you have that chemical, if you work around ammonia, butadiene and styrene, you have a right to know what the hazards of those chemicals are. You have a right to get trained in it. You have a right to get access to the material safety data sheet.

So sometimes you might not need a threshold. For our purposes, risk management I think you do need a threshold amount. I do not believe, as we have actually put in writing to the Department of Homeland Security, in the original appendix say that it had any amount. We thought that was going too far.

Ms. JACKSON LEE. Without knowing all the facts that Mr. McInnis has spoken of, but you heard him speak to the facts as he knows them: Do you believe a basic level of risk analysis, risk assessment, risk planning, proactive planning, training and accountability would have been helpful in the Goodyear incident?

Mr. MORAWETZ. I hesitate to go very far there, but just to say that something clearly went wrong. My guess is that that will be identified in the investigation, especially with the hearing that you have here today, but I don't know what that is.

Ms. JACKSON LEE. Well, simply, do you believe that something went awry to not be able to account for all employees?

Mr. MORAWETZ. That is certainly, and I think Mr. McInnis's testimony is very clear. You should have that procedure in place. If an incident happens, you should have a check-off procedure. Clearly, the situation went much too long without an adequate procedure to account for all employees.

Ms. JACKSON LEE. Would you make the argument, or at least make the suggestion, that in plants that deal with chemical elements, that such a plan and also a risk plan is very important?

Mr. MORAWETZ. Yes.

Ms. JACKSON LEE. Mr. Carafano, are you aware, or can you help us describe for the committee any Federal department that you may be aware of—agency or office—that has created an effective risk management framework? You gave us three points. Do you have any knowledge of that?

Mr. CARAFANO. Well, risk management is increasingly proliferating throughout the Federal Government. In the Army, I was actually taught risk management as a young officer. We did convoy operations and in all our military operations, we were actually given a matrix that explained how to asses risk and how to reduce risk. This was in the early 1980's. So it is not as if there aren't risk processes going on in various parts of the Federal Government.

The point is two things. I totally agree with the comment that the professionalization of risk management as a business practice in the United States is absolutely important, not just from a disaster preparedness perspective, but from a resiliency and from a sound business practice and business continuity perspective. So it is vitally important that we do that.

But I think the approach that we have to take is this is a new competency that we have become aware of actually as we have basically developed analytical tools and the ability to do this in a very kind of sophisticated way. It has to be ingrained throughout the professional development of our entire workforce in the Federal Government and in the private sector.

So this is kind of a "bigger than a breadbox" problem. It is not a point of creating risk offices and risk managers in agencies. It is about taking risk management skills, in coordination with having a professional risk management force, but in ingraining basic risk

management methodologies in professionals and managers and leaders throughout the Federal Government and the private sector.

Ms. JACKSON LEE. Let me, Mr. Paczkowski—your experience, I think, framed as you have given it in your testimony, can be very instructive for how we communicate locally, and when I say that, take what local entities unfortunately have done through tragedies that have been experienced, and begin to question or help frame how we do this at the Department of Homeland Security.

So tell us again how effective a risk management program that has been implemented at the Port Authority really is, whether or not it has grown in light of 1993 and 9/11, and to suggest whether you can do so with the backdrop of no further acts to date, but how has it mitigated, if you will, the risks that might come about because of where the Port Authority is and what it represents to those who might wish to do it harm.

Mr. PACZKOWSKI. I will echo Mr. Carafano's remarks about individual corporations and folks in the private sector, but also in the private sector agencies, taking responsibility for risk mitigation. I think it is very important. We did that at the Port Authority. We saw it as a responsibility of our agency regardless of what was done by others. We certainly began very early after 9/11 to understand the magnitude of what we were dealing with, and that risk management was the only approach we could take.

We have ingrained that process into our ongoing planning and budgeting cycle now. It is part of our education in management to really think in terms of risk mitigation. In fact, I will be in discussions later this week about an enterprise-wide risk management program to look at all kinds of corporate risk, not just those in terms of security or all hazards.

Ms. JACKSON LEE. Did you say "enterprise-wide"?

Mr. PACZKOWSKI. Enterprise-wide risk management. That is a practice that is common in——

Ms. JACKSON LEE. So you will be involved with the private sector?

Mr. PACZKOWSKI. Absolutely. In fact, as we move forward with our all-hazard risk assessment, one of the things that is essential for the Port Authority is our ports and our airports do not operate without our private sector partners. We have a very small professional cadre of public sector folks at those facilities.

Involvement of the private sector in assessing risks to those operations at those facilities is absolutely critical. How we do that, how we introduce them to the process, and how we make them partners is certainly something we are going to be cutting our teeth on in the next couple of years, but we see it as absolutely essential.

That partnership extends not only at the local level, but all the way up to the national level. DHS has done a lot in the national infrastructure protection plan to create a sector partnership model. We need to work across industry sectors to help coordinate risk management, and in the way that those sectors take responsibility for the security of their operations. I think DHS can facilitate that process much in the way it is done in the rest of critical infrastructure protection policy.

Ms. JACKSON LEE. Has the Department of Homeland Security looked closely at some of the aspects of what has been done in the private sector and utilized those? Can they do it more effectively?

Mr. PACZKOWSKI. I think they could do it much more effectively, to be honest with you. Being what I often refer to as the 9/11 agency and having spent so much effort on risk assessment, I have been rather surprised by the lack of attention we have gotten from DHS. We spend more time, frankly, with GAO in discussing our approaches to risk management.

I think that there are good models out there, not only in the public sector like the Port Authority, but also in the private sector about security risk that could very well be instructive to DHS as it advances this program.

Ms. JACKSON LEE. So we need to try to push that collaboration between DHS and the private sector?

Mr. PACZKOWSKI. Yes, ma'am.

Ms. JACKSON LEE. Let me reserve for a moment, and yield to Mr. Bilirakis for a second round.

Mr. BILIRAKIS. Thank you, Madam Chairwoman. I have a couple of questions.

Mr. Morawetz, in my opinion, much of your testimony is outside of the scope of this hearing, and many of the policy issues you raise are under the jurisdiction of other congressional committees. Explain how do safety incidents that you describe and discuss in your written testimony relate to developing a risk management framework in homeland security? Are these lessons that you believe policymakers can learn from these incidents that you describe, that will help in the formulation of risk-based methodologies in homeland security? If so, what are they?

Mr. MORAWETZ. It is a good question, but one that is a little bit difficult to answer. Let me take a step backward, though, and this is in my written testimony, and mention one of the homeland security Presidential directives, No. 8, which mentions specifically an all-hazard approach that I know some of the other members of the panel here are familiar with, that homeland security should look at all hazards, should look at terrorist threat as well as disasters such as Katrina or the flooding—I was in Cedar Rapids last week actually—or these disasters.

Maybe I got it wrong, but it seemed to me that this hearing clearly was part of it, and it was a question of the Goodyear explosion. I like to look at the field as holistically as how do we protect the infrastructure from all the hazards. The other way to look at it is I think that the very measures that you have put in proposed legislation, and some of the actions in the existing rules and regulations at DHS, of CFAS, I think can be protective of the infrastructure, whether it is a terrorist attack or whether it is a natural disaster.

I think there are things that you can put in place to minimize the effects so no matter why an incident happens—and let's take Goodyear—that you can account for all employees. That would be helpful whether it is a terrorist attack on a chemical plant or whether it is the Goodyear explosion or whether it is a facility that a tornado hits through Oklahoma.

In terms of jurisdiction of this committee, I would defer to the committee. I am not an expert on that.

Mr. BILIRAKIS. Thank you, Madam Chairwoman.

Thank you, sir.

Ms. JACKSON LEE. I just have a couple more questions. I thank you, gentlemen, and I thank the acting Ranking Member, Mr. Bilirakis, for both his contributions and his interest, and I look forward to collaborating with him on a number of important issues that we have discovered in this hearing. Thank you very much, Mr. Bilirakis.

I have a few more questions. I want to pursue your answer, Mr. Morawetz, because I think it gets somewhat muddy between safety and the word "security." I think the best way this Congress can function is to recognize that they are two very valid terms that overlap, frankly. A safe facility may be prepared for the worst, because it has all of the four corners of being prepared in place.

So let me ask you, with your experience, which reflects very importantly on security issues, can you assess how safe America's chemical plants currently are? An unsafe plant, obviously—and this is my interpretation—certainly is a great conspicuous target for terrorists. You also have the concern of chemical plants being launched, located in neighborhoods, usually residential communities are nearby.

So I would appreciate it if you would assess how safe you believe America's chemical plants currently are, and I would like you to assess whether or not you think the private sector is doing everything it can to mitigate the risk, whether it comes in the form of an unsafe incident or they come in the form of something premeditated.

Mr. Morawetz.

Mr. MORAWETZ. It is a good question, but not that easy to answer. I don't believe in painting with this huge paint brush that says this is where we are, or that we can judge it easily on a scale from one to ten.

From the facilities that I have been to, on the initial look at guns and gates, I think that the facilities are really, the ones I have seen are doing a pretty good job. I think they are looking at them. They are seeing room for improvements. I just talked to a local this week in preparation of coming that talked about gates that they were improving, the spaces, gates under railway lines, and an interesting one where at some gates that they would stop somebody and remotely let them in, but they realized that a car could easily hide behind the truck, and so they wanted to get double gates.

So there is room for improvement. I talked to a member, he said everything is going very well, but I pushed him a little bit further, and they do a lot of drills. They do a couple a year, far beyond what the mandates of any regulation is now or even proposed. But I asked him further, well, what about all the shifts? It turns out since salary, of course, is mainly on first shift, the drills were only on first shift. I think that is a point he will bring back to management, and I think it is a process back and forth.

So my impression is of the facilities I have seen is that they are somewhat secure. Does that mean that all the procedures are in place that can minimize the risk? I am not sure. I would say that

clearly from my example there is room for improvement, but it is hard otherwise to paint the broad brush.

Ms. JACKSON LEE. Would you just, if you will, philosophize or stretch your analysis that a safe plant would also have procedures in place that would be equally responsive in light of a potential terrorist attack? If a plant had risk procedures in place, accountability, accounting, evacuation procedures in place, that would translate potentially if the incident was provoked by an accident or provoked by something premeditated?

Mr. MORAWETZ. I think that is exactly correct.

Let me just add one other point, beyond my direct experience, you mentioned before the Chemical Safety Board. There still are these accidents. There still are these investigations. It is not just Goodyear that happened or hydrogen sulfide in Cincinnati. These incidents do happen.

So the question is, is it just that they are going to happen? Or are there steps that we can take reasonably to protect them?

Ms. JACKSON LEE. Mr. McInnis, you have served in this industry for some I believe 38 years. Is that accurate?

Mr. MCINNIS. Yes, ma'am.

Ms. JACKSON LEE. Certainly, your service pre-dates the horrific tragedy of 9/11, meaning that you started working before we had an idea of terrorist attacks in the United States. Is that right?

Mr. MCINNIS. Yes, ma'am.

Ms. JACKSON LEE. This is an appropriate moment to thank your son for his service in Iraq. We thank the sergeant very much, and we honor him, and we offer our sympathy to him and other family members. But I am glad you recounted the story of how hard it was for him to get back and how he needed to get back for is mom. It was our honor and pleasure, I know.

Mr. MCINNIS. He thanks you both very, very much. I am relaying that message from his heart and mine, the family.

Ms. JACKSON LEE. We are honored with his service.

So let me just go back to having been in this business for 38 years. Can you tell us how worker security and safety has changed since you started telling about training and staff cuts and things that might have impacted? What do you see are the missing elements? What is missing in what you have seen since you came into the plant?

Mr. MCINNIS. Well, in the past every facility that had manpower in it had a supervisor, which I say would be the leader in charge. The day shift had a lot more supervision. They had more personnel, and the fire department was fully loaded. Everything was proper. They had a procedure. I don't think we had too much. It was small drills, little fires, and everything went smooth.

But in the past 14 years, I would say, before I started to leave, this was Goodyear's goal to cut everything. They used this threat for contracts. They were going to do away with jobs or they were going to shut the plant down. So the people who needed a job took these cutbacks in wages and jobs so they could have a job to support their families. They would sign these.

Take for instance the fire department. I will tell you how it is staffed now. Before, it was staffed 24 hours a day. Now, they have two to three firemen per se each day, and the backshift, which is

anything after 3 o'clock, they have none, they have nobody. Then because of the cuts you go to the EMS or emergency response teams, there is no set pattern on those. You may run across a shift that may have eight individuals working in the medical, and another shift may only have one or none.

So what I am saying is now, with just a shift foreman himself running the plant on backshift, he is by himself. So if he had a disaster by himself, it would be worse than what happened 2 weeks ago.

Ms. JACKSON LEE. Did you make the point that your wife, who was also a dedicated employee, was in essence stretching herself helping out somewhere else where it seems that you said she didn't have to be there, but she was helping out. Could you explain that?

Mr. MCINNIS. Yes, ma'am. Like I said, we discussed that many times, and that was one of the things we talked about, that she would come home exhausted because her job was in one end of that plant, and they would call her or she would volunteer to go up. I spent many a day talking to her on the phone, and I would hear them calling and saying, "Can you come help us?" They don't have the personnel.

The supervision has been cut to a bare minimum, and that is why she went to those areas. She didn't have to go. What I am saying is these cuts by the company has caused—you know what I am talking about. It just caused this incident itself because she wouldn't normally be there.

Ms. JACKSON LEE. So the worksite where she normally works, was that impacted by the incident? Or would she have been in a safe area or been able to evacuate? Do you know?

Mr. MCINNIS. I am sorry, ma'am. I missed the first part.

Ms. JACKSON LEE. The area where she traditionally worked, where she had to leave and go to that part of the plant, would she have been away from the incident if she had been where she traditionally worked?

Mr. MCINNIS. Yes, ma'am. There is another plant between where this explosion occurred and where she worked. So there was a whole other plant between that situation where her job really was.

Ms. JACKSON LEE. Thank you, Mr. McInnis.

Dr. Carafano, in your testimony you mentioned that it is not necessary for issues pertaining to pandemics or energy supplies to be elevated to national security status. Can you please elaborate on this? How should the Government then address these issues?

Mr. CARAFANO. Yes, ma'am. The problem with labeling things as national security issues is that automatically does two things. When you say something is a national security issue, it means that we intend to invest our Federal authorities with enormous power and responsibility. The preamble of the Constitution says that providing for the common defense is fundamentally the Government's job.

So when you do that, you have a tendency to over-Federalize, over-centralize and make Government very intrusive in your life. So we do that for basically threats of other malicious actors, whether they are state or non-state actors, threatening the United States. It doesn't mean there aren't other problems and they don't rise to the level of national importance, but when you start to call

them national security issues, you are in a sense ceding all kinds of authority to the Federal power, and I think we want to be very cautious about doing that under any circumstances.

The second thing is when you call something a national security problem, the tendency is to look for a national security solution, so the tendency is to default to national security instruments such as the military or such as, again, having DHS do this. So I think we should be very cautious in what we call a national security issue. In my mind, the only thing that rises to the level of a national security issue is a state or non-state external threat who is threatening the stability and the coherence of the Nation. Other issues are national issues which we should certainly address, and they can be national issues and national priorities, but we shouldn't call them national security issues.

If I could just follow up very quickly, I just wanted to go back to the excellent point that you made, and I think a point that we all should account for, and that is what is the most effective way to instill risk assessment in the private sector and the public sector. You brought up a really excellent point about employee involvement in disaster planning and business continuity.

The data on this is absolutely really clear. There is a tremendous researcher up in New York, Roz Lasker, who has done a lot of work on this. She has compared emergency planning for communities where it is done by professionals, and then where it is done with the input of people in the community. The answer is exactly the same in the workplace. When the people in the workplace participate in the planning, No. 1, you get much better buy-in because they are part of the planning process; and No. 2, you get much, much better plans.

So emergency and disaster planning which integrally includes the workforce and the people in the planning process is infinitely better and stronger. We know that. The data suggests that. So how do we get people to start doing this? I go back to the point I made before about the SAFETY Act. For example, one of the things you can do under the SAFETY Act is you can give SAFETY Act protections to risk management processing, management and planning.

So for example, a good company that has a good risk management product, they would include in that risk management assessment, did you bring the workforce into making that plan? Then a company that would use that risk management, that got SAFETY Act protection, you know, a company might be incentivized to use that risk management process and to integrate it into their business practices and a business continuity plan. Then you get a stronger, better plan for that.

So I do think we need to look at things like the SAFETY Act, where we can really incentivize people to adapt best practices, which are in the end going to save lives, prevent tragedies like this from happening, allow businesses to operate better and more efficiently, and be more resilient in the face of disasters.

Ms. JACKSON LEE. Well, let me say, I appreciate the importance of both my question and your answer, which is that we need collaboration. We need to be able to focus on ensuring that the private sector is in tune with risk assessment and risk management.

But let me tell you why we need to be sensitive to the question of national security. I don't believe that the solution to national security is always the military, but I would like to think that it is preparedness and that it has some home in the Department of Homeland Security. My example is such. Prior to 9/11, our focus was not on the vulnerability per se of tall skyscrapers. We admired them. We toured them. We didn't have much of a focus on them.

In fact, as my recollection serves me, the towers built in the 1970's had a different approach in terms of how they were structured. They thought they were meeting the test of what could happen. They could not predict or did not predict a forceful missile coming in with how many tons of fuel. So in essence, entities have now come under the umbrella of national security, i.e. airports, because we have been awakened to the possibility of a national security through airports and airplanes.

So I think we cannot limit our thinking in that. I will give you a chance to answer it, but I am going to go to Mr. Paczkowski. Do you see where I am going on that? I think you have lived in the World Trade Towers, or you really know them. Doesn't our risk assessment, and particularly from local governments and local entities, have to take into consideration the risk, if you will, of nonthreatening entities becoming unfortunately a tool of terrorism? Do we have to take that into account in our preparedness and our risk assessments?

Mr. PACZKOWSKI. I think we have become a lot smarter, that we need to take a more holistic look at a full range of threats. I think when we think about risk assessment, and I agree with Mr. Carafano that a lot of the dialog has been on mitigating a vulnerability. We have focused an awful lot of attention on the very moment we think someone is going to show up with a bomb at our facility, and not enough attention on all the things that might in fact prevent that from happening, so focus on prevention, and also building into in particular our infrastructure and our key resources the kind of ability to withstand an impact over the long term, the resilience that we need to build into our systems.

Ms. JACKSON LEE. But don't we need to look at ports and airports and trains with a different eye than we previously look at them?

Mr. PACZKOWSKI. Absolutely. I mean, if you were to ask questions of the Port Authority in 1990, let's say, you know, you would get a very different answer than you would get today. We certainly do feel that we are on the frontlines, if you will, of this security challenge.

Ms. JACKSON LEE. Let me ask Mr. Morawetz just a question about helping employees to be part of the safety. Is it helpful that employers give to employees both risk assessment plans, but also records of previous incidents? You may be a new employee or you may be a longstanding employee, but you have the ability to access those records.

Mr. MORAWETZ. Well, in terms of incidents, there is the OSHA log, so certainly any serious injury or fatalities would be part of the OSHA log that is posted and the union has a right to it.

Ms. JACKSON LEE. But this would be incidents that may not have resulted in injury, but it occurred. Should employees have the ability to have access to that?

Mr. MORAWETZ. I think they should, and I think that that can be invaluable information as part of the communication back and forth, as Dr. Carafano said. Two things happen. No. 1, you get additional information from a wide variety of people who work at an institutional workplace, but No. 2, you get the buy-in, you get the ownership. So I think people will then implement the plan.

Ms. JACKSON LEE. You may get ideas on how you can avoid it.

Mr. MORAWETZ. Yes.

Ms. JACKSON LEE. What about whistleblower protection for employees?

Mr. MORAWETZ. I think that is a fact of life, that people feel scared on the job. It was part of my testimony, and I think that having whistleblower protection is important. It may never be used, but in an instance where people need it, it should be in place.

Ms. JACKSON LEE. I hope that that translates to making, in your opinion, a safer plant.

Mr. MORAWETZ. Yes, it does, because the information won't come forward. If the information or weakness doesn't come forward, then the weakness may not be seen and won't be corrected.

Ms. JACKSON LEE. Dr. Carafano—we call you "doctor," and I see "mister." I want to correct the record.

Mr. CARAFANO. [OFF MIKE]

[Laughter.]

Ms. JACKSON LEE. And humor. Are you a doctor?

Mr. CARAFANO. I am a doctor.

Ms. JACKSON LEE. All right. We will correct the record. It is Dr. Carafano.

Did you want to comment briefly? I am going to let Mr. McInnis have the last word.

Mr. CARAFANO. Thank you, Madam Chairwoman.

You know, you made an absolutely excellent and critical point. Before 9/11, we grossly underestimated vulnerabilities in this country. That is true. The point is, we also grossly underestimated threats, and we also grossly underestimated criticality. If you want to walk the walk of risk assessment, you have to have a holistic discussion that balances all three.

Today, we focused on a lot of really valuable issues, but we virtually only talked about mitigation and vulnerabilities. We really didn't have a discussion about criticality and about threat reduction. You have to combine all three of those if you really want to do serious risk assessments.

Ms. JACKSON LEE. My answer to that, Dr. Carafano, is the first panel. That is what we were proposing to the Department of Homeland Security. That is their responsibility. That is the necessity of a chief risk officer. That is a need for getting a baseline and for quarterly meetings, for giving us their minutes, to get where you need us to be.

We had to highlight what happens, unfortunately. Mr. Paczkowski is an example of what happens when we were, in essence, not informed. I will put quotes around "asleep at the wheel" because I know there are many hard-working people in a certain

instance. So your testimony and what you have just allowed us to understand is a guidepost for what we believe the Department of Homeland Security must do to impact on our plants as it relates in all instances security, but we have to also overlap on safety, because any vulnerability projects us into the 21st century for what we know can happen as it relates to terrorism.

So you are very right and you have just posed the questions that we are demanding of the Department of Homeland Security as evidenced by my earlier questions to that panel. We do thank you.

Mr. McInnis, I will pose the last question to you. I am giving you the last word, inasmuch as you have come in this time of need and also a time of concern.

How much concern should we have? You are an experienced plant worker. You are not all over America, but how much concern should we have for the plants in America if the trend that you have discussed, the losing supervisors and losing employees and lack of training prevails? How much concern should this committee have?

Mr. MCINNIS. Ma'am, there should be plenty for the simple reason, as I mentioned earlier, all these things are slid by. I sat back and watched years ago when OSHA would come by with a small slap on the wrist. It is posted and everybody knows it. But these things don't bother people.

Getting to the accidents happening, and security as far as that goes: If you are cutting the personnel, you are cutting your own throat. You have these people sitting up there in Akron, as I said, making these changes, and these poor individuals down here happen to work under those conditions. It affects the safety and security of the plant.

Like I mentioned, the fire department, the EMS or emergency response teams, and the security is—I know we don't have time, ma'am. I can go over issues of those things that happened over the years that I personally tried to change myself. But there again, it comes from up above what goes on.

My thought on this particularly, and I thought about this today, Enron goes to jail for fraud of the people. What happens when somebody is killed in a plant because of unsafe conditions and everything? What happens to them? I think these people need to go to jail. Forget the fines. Let's put them in jail and see if this will change their philosophy as opposed to wanting greed and wanting money. It might slow them down and do the right thing.

Ms. JACKSON LEE. Well, Mr. McInnis, you may have just made yourself a consultant to this committee as we go forward for the many issues that you know about. I think all the witnesses have made this hearing a good first start, or a continuing of what we are trying to achieve in the Department of Homeland Security, which is the understanding of risk assessment, risk management, and the roadmap that we need to take, Mr. Paczkowski, to make your job easier and to create that collaboration that you have spoken of, and certainly for Dr. Carafano to ensure that we do reach those aspects that you mentioned, and to Mr. Morawetz, that we have the kind of plant system across America that is befitting of this 21st century Nation.

I thank all of the witnesses for their testimony. If you would just wait a moment so that I can get the appropriate language into the

record for my committee Members. I want to thank the witnesses for their valuable testimony and the Members for their questions. The Members of the subcommittee may have additional questions for the witnesses. We would appreciate it if you would answer them expeditiously, and we ask that they come both expeditiously and in writing.

Hearing no further business, the subcommittee stands adjourned.

[Whereupon, at 5:33 p.m., the subcommittee was adjourned.]